DoD CIO

Annual

Information Assurance

Report

April 2000

**Office of the Assistant Secretary of Defense
Command, Control, Communications, and Intelligence**

Form SF298 Citation Data

Report Date ("DD MON YYYY") 01042000	Report Type N/A	Dates Covered (from... to) ("DD MON YYYY")

Title and Subtitle DoD CIO Annual Information Assurance Report	Contract or Grant Number
	Program Element Number
Authors	Project Number
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Office of the Assistant Secretary of Defense Command,Control,Communications,and Intelligence	Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)	Monitoring Agency Acronym
	Monitoring Agency Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract

Subject Terms

Document Classification unclassified	Classification of SF298 unclassified
Classification of Abstract unclassified	Limitation of Abstract unlimited
Number of Pages 127	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 4/1/00	3. REPORT TYPE AND DATES COVERED Report

4. TITLE AND SUBTITLE
DoD CIO Annual Information Assurance Report

5. FUNDING NUMBERS

6. AUTHOR(S)
Not provided

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Information Assurance
Technology Analysis Center
(IATAC)
3190 Fairview Park Drive
Falls Church, VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical
Information Center
DTIC-AI
8725 John J. Kingman Road,
Suite 944

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE

A

13. ABSTRACT *(Maximum 200 Words)*

This report reflects 1999 accomplishments and describes numerous activities underway in the information assurance (IA) arena. The sheer number and scope of activities in 1999 demonstrate DoD-wide commitment and concern for IA, as well as across-the-board awareness of the shared risk environment. Many of the activities are new for some of the Components and will pave the way toward future successes.

14. SUBJECT TERMS
IA

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT Unlimited

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

THIS PAGE INTENTIONALLY LEFT BLANK

COMMAND, CONTROL,
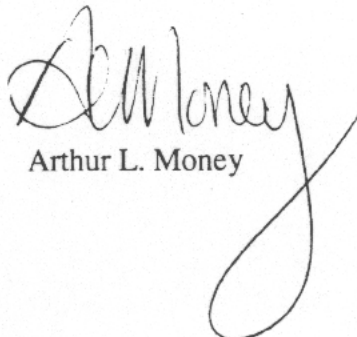COMMUNICATIONS, AND
INTELLIGENCE

April 12, 2000

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: 1999 DoD CIO Annual Information Assurance Report

Section 1043 of the National Defense Authorization Act for Fiscal Year 2000, Public Law 106-65, tasked the Secretary of Defense to submit an annual report on the Defense Information Assurance Program.

The attached report reflects 1999 accomplishments and describes numerous activities underway in the information assurance (IA) arena. The sheer number and scope of activities in 1999 demonstrate DoD-wide commitment and concern for IA, as well as across-the-board awareness of the shared risk environment. Many of the activities are new for some of the Components and will pave the way toward future successes.

My point of contact for this report is CAPT J. Katharine Burton, USN, Defense-wide Information Assurance Program (DIAP) Staff Director, telephone 703-602-9988, email: katharine.burton@osd.pentagon.mil.

Arthur L. Money

Attachment

cc:
Deputy Secretary of Defense

Contents

THIS PAGE INTENTIONALLY LEFT BLANK

Figures

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

Today's globalization of systems and networks creates a new dimension for warfare. The adversary can be a lone hacker either out for a thrill or with a grudge against the U.S. government, a member of a state-supported cyber-warfare group, or a cyber-terrorist driven by ideology, religion, or money. The new warfighter is the cyber-warrior with technical and non-traditional skills. Complicating this new "dimension" is the need for the Department of Defense (DoD) to change its defensive strategy, because of cost and complexity issues, from the risk-avoidance approach to the risk management approach.

Information assurance (IA) has emerged as a critical component of DoD operational readiness, providing the means to detect, react, and restore vital services—as efficiently and effectively as possible—following intrusions or attacks from the outside or from within. This year saw DoD continuing to make major improvements in its IA posture—but with some troublesome issues remaining for senior Defense leaders.

This report describes recent DoD initiatives and on-going activities, their accomplishments, and issues. These initiatives and activities are consistent with those outlined in three previous reports[1] to Congress from the Secretary of Defense (SECDEF).

Introduction

Until only a few years ago, concern for the security of the information and information systems of DoD existed only within the national security community, primarily addressing classified information. As the Department networked its activities and automated many functions, the concern for information and information systems expanded to include not only classified information but also sensitive unclassified systems and information that were becoming increasingly critical to the ability of the Department to achieve its mission. Numerous Government Accounting Office reports, DoD Inspector General reports, and DoD-sponsored studies—both internal and external—pointed out deficiencies and vulnerabilities in the protection of these systems and the information contained within. Exercises, such as Eligible Receiver, and real-world incidents, such as Solar Sunrise, have also reemphasized the vulnerability of many of our systems to attack or infiltration.

As DoD began to address these vulnerabilities, the complexities of the issues became apparent, along with the necessity to change how DoD approached the problem. Initial activities provided only partial, and less than satisfactory, answers and reinforced that a multi-pronged approach—people, operations, and technology—was the only real answer. Progress would be slow and many missteps could occur, but work began throughout DoD.

---

[1] DoD CIO Annual Information Assurance Report, May 1999; Assessment of the Information Assurance Program of the Department of Defense, May 1998; and Report to the Congress on the Information Security Activities of the Department of Defense, December 1997.

FY99 Advances

The past year has been one of significantly increased activity in the IA arena. Investments and programs initiated in previous years were beginning to show excellent results, with progress being made in addressing complex issues. In the 1998 DoD Annual IA Report, we described eleven major initiatives as well as activities at six Components. In this document, we report on twelve major DoD-wide initiatives, activities at fifteen Components, as well as activities at the unified and specified commands and three special-interest communities.

Several issues addressed in the 1998 report are not reported in a separate section but are included in the report of the component with primary responsibility. Two keys issues so reported are the National Security Incident Response Center and the Joint Task Force Computer Network Defense. The sheer number and scope of activities in 1999 demonstrate not only DoD-wide commitment and concern for IA but also a major increase in awareness at all levels and in all DoD activities of the shared-risk environment.

In the following sections, we briefly summarize some key Defense IA Program activities in Fiscal Year (FY) 1999. The reader should refer to the individual sections in the main body for a more detailed discussion.

DoD PKI Policy

On May 6, 1999, Dr. John Hamre, the Deputy Secretary of Defense (DEPSECDEF), issued a formal DoD Public Key Infrastructure (PKI) Policy. This policy emphasized the importance of achieving Information Superiority[2] in a highly interconnected, shared-risk environment by requiring that DoD IA capabilities address the diversity and pervasiveness of information, information systems, and infrastructures to support warfighting and business operations as part of DoD's Global Information Grid (GIG).

IA Training and Certification

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) jointly commissioned the IA and Information Technology (IT) Human Resources Integrated Process Team (IPT) to (1) identify the critical IA and IT management skill sets in DoD and (2) recommend mechanisms to promote the achievement and sustainability of those skills in the Department. The team's final report presented 19 recommendations to improve the way in which the Department manages its IT workforce, with 12 of the 19 directly affecting IA training and certification.

DoD Computer Forensics Lab (DCFL)

DoD officially opened the DCFL, a state-of-the-art facility to process computer evidence in criminal, fraud, and counterintelligence investigations for the all of the Defense Criminal and Counterintelligence Investigative organizations. DoD also convinced the Federal Bureau of

---

[2] As defined in Joint Vision 2010, information superiority is "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."

Investigation (FBI) to build a computer forensic capability that is co-located with the DCFL, the first of many efforts to leverage other criminal investigative organizations.

Insider Threat Integrated Process Team

ASD(C3I) established the Insider Threat IPT to recommend actions and policies that would minimize the impact of the insider threat and, failing that, minimize the potential damage to DoD information or inflicted on DoD information and information systems by significantly reducing the vulnerabilities of DoD information systems. The IPT has identified a strategy and a wide range of choices currently available to satisfy the objective.

Computer Network Defense

The Office of the Assistant Secretary of Defense (OASD)(C3I) established a Computer Network Defense Working Group (CND WG) with representation from the Joint Staff, Commanders in Chief, Military Services, Defense Agencies, and Intelligence Community, and coordinated with related working groups and IPTs. The CND WG identified the core functions of CND; developed a CND framework; and produced a draft DoD Directive for Computer Network Defense and Program Objective Memorandum Preparation Instructions for the FY02-07 Planning, Programming, and Budgeting System cycle.

IA Research

The Information Systems Security (INFOSEC) Research Council (IRC) coordinates, collaborates, and influences IA research within DoD (specifically the Defense Advanced Research Projects Agency, the National Security Agency, and the Military Services) as well as with other organizations such as the Department of Energy, the National Institute for Standards and Technology, and the Central Intelligence Agency. The IRC developed a "hard" problems list to help focus IA research efforts, ranging from intrusion/misuse detection and response to influencing vendors. This year, the IRC rolled out its database that answers the question "Where is the DoD Community spending IA research dollars?"

IA Vulnerability Alert (IAVA)

Recent network assessments and external activities continue to demonstrate that widely known vulnerabilities - with the potential to severely degrade mission performance - still exist throughout DoD networks. IAVA has been highlighted through a Deputy Secretary of Defense Memorandum[3] as one approach to inform all DoD elements about vulnerabilities. DISA's new database, the Vulnerability Compliance Tracking System (VCTS), can immediately distribute vulnerability information to each system administrator and track and report on their responses to these alerts. Prototypes of VCTS have been developed at U.S. Southern Command, U.S. Space Command, and U.S. Joint Forces Command.[4]

---

[3] Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Information Assurance Vulnerability Alert (IAVA)," December 30, 1999.

[4] Formerly the U.S. Atlantic Command.

Reserve Component Study

OASD for Reserve Affairs, (Research, Training, and Manpower) (RA(RT&M)) chartered a study to identify IA missions for the Reserve Components (RC) in support of mission requirements assigned by DoD. The study team developed recommendations for specific actions that ASD(RA) could pursue in which the RC could make positive and immediate contributions to the IA posture of DoD.

Global Information Grid (GIG) IA Guidance and Policy Memorandum

GIG[5] covers all major aspects of information technology including computing, communications and networks, interoperability, technology, resources, and IA. The proposed IA guidance and policy memoranda (G&PM) addresses not only the confidentiality requirement of DoD's information but also its availability, integrity, and the need for strong identification and non-repudiation services. The GIG IA G&PM incorporates the Defense-in-Depth (DiD) strategy described in last year's IA annual report, and establishes a closer working relationship with the Intelligence Community.

Web Security Initiative

Unclassified and innocuous information on Websites, when combined with other sources, may increase the vulnerability of DoD systems and endanger DoD personnel and their families. The Deputy Secretary of Defense issued guidance[6,7] addressing these vulnerabilities and directed several actions. A DoD Directive and Manual are in preparation. The Deputy Secretary of Defense approved the Concept of Operations for the Joint Web Risk Assessment Cell.[8]

Defensive Information Assurance Red Team

OASD(C3I) developed an IA red team methodology through a collaborative effort involving many of the red team organizations within the IA community. The Defense-Information Assurance Red Team (D-IART) methodology focuses on DoD requirements while its companion document, the Information Assurance Red Team Handbook, is suitable for use throughout the government.

IA Architectural Overlay

Achieving affordable systems that meet various mission needs and that are protected is an extremely difficult and complex task. Compounding this problem is the evolution of existing applications to make them more integrated, more distributed, and more widely interconnected. OASD(C3I) convened a small quick-reaction IA Architectural Working Group to recommend a course-of-action and its implementation.

---

[5] GIG was first called the Global Networked Information Enterprise (GNIE) initiative.

[6] September 24, 1998.

[7] Website Administration Policies and Procedures, December 7, 1998.

[8] February 12, 1999.

Component Initiative

In addition to participating in Defense IA Program activities, each Component took further initiative for their specific and individual needs in 1999. Their many efforts contribute to assuring the DoD IA posture and represent a significant, cumulative benefit toward the objectives of the Defense-wide Information Assurance Program (DIAP).

IA Resources -- Investment Review

To gain better insight of the totality of IA resources, the Department began conducting a zero-base investment review of the principal Program Element (PE) that funds IA advance and operations. The effort will continue in order to extend and refine this resource visibility beyond this critical PE and develop additional knowledge to support the oversight responsibilities of DIAP.

Going Forward

Much work remains to be done. Many of the activities in this year's report are new on the part of many of the Components, and the next few years will demonstrate how successful these activities are as well as how to integrate them into the operations of the Department.

We expect that as Y2K efforts wind down, additional attention and resources will be focused on IA efforts. Progress cannot stand still—as the complexity of our systems continues to grow, so do both our vulnerabilities and the sophistication of our opponents in exploiting our weaknesses. In addition, our efforts in partnership with other Federal agencies, with commercial and private entities, and with our treaty and coalition allies, will determine our success in protecting our information and information systems.

THIS PAGE INTENTIONALLY LEFT BLANK

1. Introduction and Summary

1.1. Background

Information Assurance (IA) is defined as:

> "Information Operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities." (DoD Directive S-3600.1, "Information Operations (IO) (U)," December 6, 1996.

IA has become the Department of Defense's (DoD) second highest priority issue, with only Y2K of higher concern. DoD is increasingly dependent upon a commercially based global information environment over which it has little control, thereby increasing the Department's exposure and vulnerability to a rapidly growing number of sophisticated internal and external threats. Today's inter-networked information systems make it possible for an adversary to surreptitiously disrupt many systems, networks and users by gaining access to a single network connection. Once inside a system, an adversary can exploit it and the systems networked to it. This global marriage of systems and networks creates a shared-risk environment and a new dimension for warfare, one in which the warfighter is now a cyber warrior with technical and non-traditional skills rather than a traditional platform-based individual who relies only on a tank, ship, or aircraft.

IA provides the means by which cyber threats are countered. IA has emerged as a critical component of DoD's operational readiness. IA enables the systems and networks composing the Defense Information Infrastructure (DII) to provide protected, continuous, and dependable service in support of both warfighting and business missions. IA relies on a risk-management blend of managerial, procedural, and technical activities that work toward assured availability, integrity, authenticity, confidentiality and non-repudiation of information services, while providing the means to efficiently reconstitute these vital services following an attack. It includes an extended focus on DoD missions and infrastructure that are substantially interwoven with our National Information Infrastructure and increasingly dependent on services derived from the Global Information Infrastructure.

The Department continued to take major steps in 1999 to improve its IA posture. This report describes recent DoD initiatives and the ongoing activities required to meet current and future DoD and national IA challenges. These initiatives and activities are consistent with those outlined in three previous reports to Congress from the Secretary of Defense.[9] They support Presidential Decision Directive (PDD) 63, "Critical Infrastructure Protection," May 22, 1998, and numerous additional reports and studies listed in Section 4 of this report.

---

[9] The reports are the DoD CIO Annual Information Assurance Report, May 1999; the Assessment of the Information Assurance Program of the Department of Defense, May 1998; and the Report to the Congress on the Information Security Activities of the Department of Defense, December 1997.

1.2. Objectives of the Defense IA Program

The goals and objectives of the Defense IA Program are formally promulgated in the DoD Information Management (IM) Strategic Plan, version 2 which clearly ties IA to Information Superiority. Goal Four of the IM Strategic Plan details the specifics of the Defense IA program as:

Goal 4 Ensure DoD's vital information resources are secure and protected.	Information Authorized Access Unauthorized Access
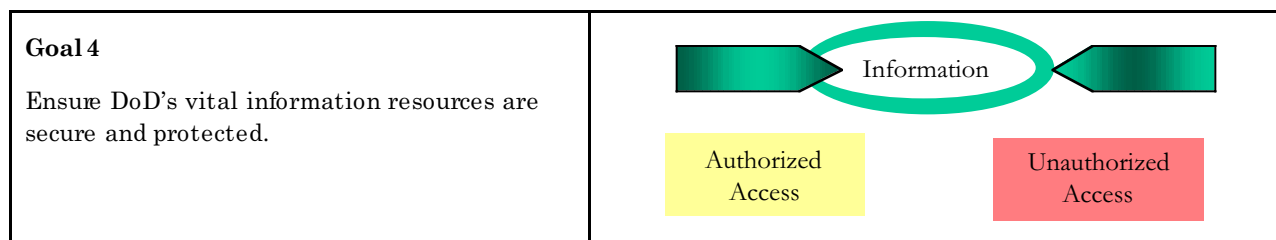
Description

The capability of DoD to execute its mission from peacetime through conflict and a return to peacetime is highly dependent upon the interconnected set of information systems and networks called the DII and the expanding national and global infrastructure. In today's environment of sophisticated weaponry and rapid global force projection requirements, the ability to provide timely, accurate information is vital to all aspects of DoD operations. Indeed, Information Superiority is at the very foundation of our vision of modern warfare, and IA is essential to achieve and maintain information superiority. IA is an integral part of Joint Vision (JV) 2010 and the ability to integrate intelligence, command and control, and battlefield awareness functions into joint and combined operations. IA is also an essential element to implementing protection of critical national infrastructures mandated by the PDD – 63, Critical Infrastructure Protection.

This view emphasizes the importance of IA to the Department's warfighting capability and recognizes the need to integrate IA into all facets of military operations. Such integration involves more than simply acquiring IA technology. It requires improving the awareness of individuals throughout the Department of both the criticality of information operations and the role of IA in support of operational missions. Most importantly, it requires a clear operational understanding of the risks and impacts of an inadequate IA posture on defense missions. This perspective will require a significant cultural change in the approach to IA across the Department, one that recognizes IA as a warfighting concern and ranks it appropriately in Departmental attention and budgetary tradeoffs with other warfighting capabilities. Attaining increasingly effective yet affordable IA capabilities requires operational attention and a continuous improvement process that incorporates assessments of both risk and return-on-investment.

A robust IA program requires:

- effective operational policies and doctrine;

- appropriate technology, tools, and materials;

- a corps of professionals educated and trained in IA;

- continuous monitoring and assessment of threats, vulnerabilities, and readiness posture;

- the ability to quickly and efficiently implement agency-wide security measures and countermeasures to limit damage when threatened; and

- appropriate management and oversight.

The Defense IA program includes specific goals and a strategy to guide the Department's activities and ensure the vision of Information Superiority is achieved. The goals focus on:

- protecting mission critical information, whether classified or using risk management techniques;

- furnishing robust systems and reconstitution when required; and

- cultivating a cadre of IA professionals.

The underlying strategy to achieve these goals is process oriented and based on the principles of risk management, continuous improvement, and performance-based investment. It reflects:

- the strong link of IA to operational readiness;

- the need for continuous monitoring and reporting of the Department's IA posture;

- the use of the DoD Chief Information Office (CIO) organization and management processes to address IA;

- a Defense IA Program that provides the planning, coordination, integration, and oversight of the Department's IA resources and investments; and

- an awareness on the part of all members of the organization of the distinction between information that is operationally sensitive and information that can be made available to the public.

This approach must also address the information infrastructure vulnerabilities, physical as well as those open to cyber attack. The disruption, failure, or destruction of equipment or services (e.g., power, cooling, telecommunications) that support the information infrastructure have the potential to disrupt critical services just as much as cyber intrusion.

The Department's IA improvement efforts are guided by the objectives and strategies contained in the IM Strategic Plan, Goal Four; located in Annex 5.

1.3. DoD Strategy in Meeting Objectives

Defense-in-Depth (DiD) is the strategy the DoD is pursuing to ensure success in both cyber warfare and warfare dependent upon information superiority. Figure 1 depicts the components of this strategy.

- **Operations.** IA policy drives IA operations by establishing goals, actions, procedures, and standards. IA policy formally states the security requirements in terms of what must be done and not done. Policy establishes standards that define uniform and common features and capabilities of security mechanisms, the rule or basis by which to measure the various dimensions of IA, and the desired or required level of attainment.

- **Personnel.** People, using technologies to conduct operations, are the central element of DiD. People design, build, install, operate, authorize, assess, evaluate, and maintain protection mechanisms.

- **Technology.** To conduct an effective cyber-defense, DoD must have a well-stocked arsenal of technological weapons and the skills to use them. DoD has greater confidence in the effectiveness of the technology tools and products used in DoD IA solutions because they must be evaluated under programs designed to assure their utility and capability.
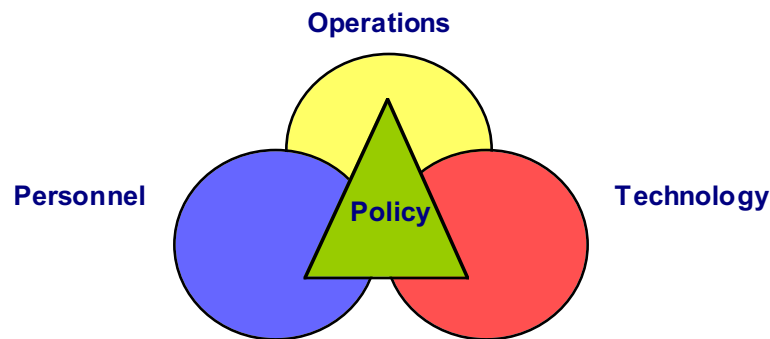
Figure 1. Objectives

General. Modern warfighting is network-centric. Without secure and non-secure networks (such as SECRET Internet Protocol Router Network (SIPRNET) and Sensitive unclassified Internet Protocol Router Network (NIPRNET) modern forces cannot accomplish their assigned missions. Because of its importance, the network itself is a weapons systems that enables the application of kinetic forces by providing:

- targeting, threat, and electronic order of battle information;

- navigational data and timing;

- weather predictions;

- weapons availability, fuel, spare parts and other logistical support;

- dissemination of the air tasking order, mission reports, and other vital command and control; and

- health and morale support of deployed forces.

This network eases force protection concerns by allowing the forward deployment of only those personnel absolutely necessary. Those personnel then "reachback" to rear echelons

for critical support information—and information systems and the network are the weapons systems that allows this to occur quickly, efficiently, and securely. Therefore, this network is truly global and now referred to as the Global Information Grid (GIG). The operation of the network is the primary means of employing the GIG. Effective network operations requires the full integration of its three pillars, Information Assurance, Information Dissemination Management and Network Management, as depicted in Figure 2.
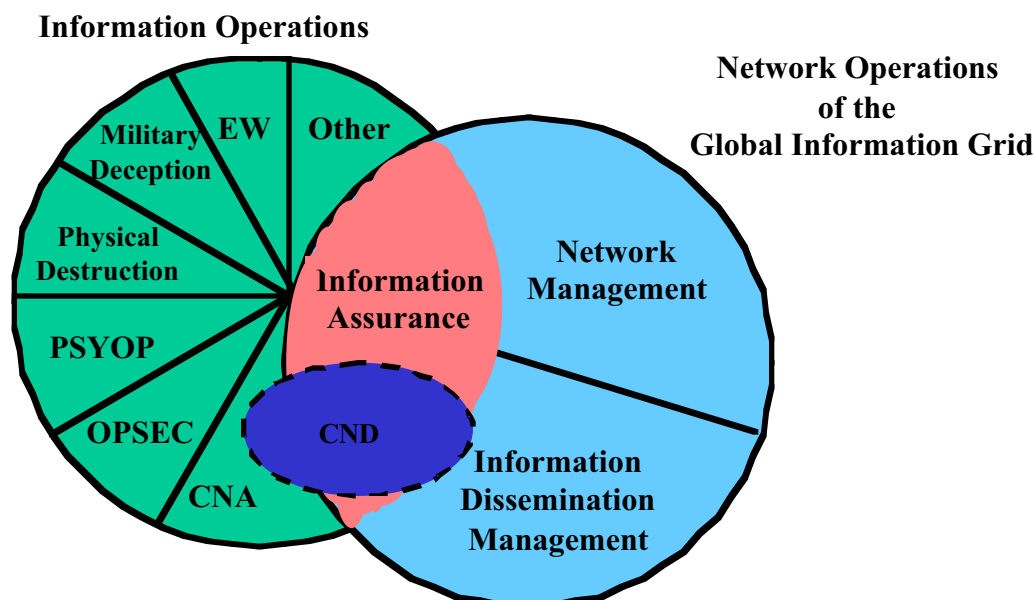
Figure 2. Information Operations and Network Operations of the Global Grid

Just as IA is a part of network operations, Figure 2 also shows how IA is a part of Information Operations, along with Electronic Warfare, Military Deception, Physical Destruction, Psychological Operations, Operational Security and Computer Network Attack and Defense. As seen in this figure, Computer Network Defense is nearly synonymous with IA and clearly plays a large role in network operations. The same warfighters whose mission is IA are also experts in defending computer networks. And in a world where nearly every device contains a computer, and the vast majority of them are networked together, the boundaries between these two mission areas are becoming indistinguishable.

IA through DiD. IA is critical to the military's ability to conduct warfare and is the responsibility of all modern warfighters. Because of the global nature of the global information grid, a risk assumed by anyone at any level is a risk assumed by all. Therefore what is required is IA at all levels and the method to employ that is through the concept of DiD which employs mechanisms on successive layers at multiple locations. To prevent the potential breakdown of barriers and the invasion of the innermost (or most valuable) part of the system, we must construct our defenses in successive layers by positioning safeguards at different locations. These different locations are expressed as networks, enclave boundaries, local computing network and supporting infrastructures. Through a deliberate risk analysis process, leadership can make effective risk-management decisions on how to best deploy the appropriate DiD strategy.

IA fundamentals. IA actions are part of Information Operations that incorporate protection, detection, and reaction capabilities to protect and defend information and information systems. The fundamental pieces of IA are:

- **Availability**. Timely, reliable access to data and services for authorized users.

- **Identification and Authentication**. The process an information system uses to recognize an entity. Authentication is a security measure designed to establish the validity of a transmission, message, or originator, or as a means of verifying an individual's authorization to receive specific categories of information.

- **Confidentiality**. Assurance that information is not disclosed to unauthorized persons.

- **Integrity**. Protection against unauthorized modification or destruction of information.

- **Non-repudiation**. Assurance that data being sent is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

1.4. Summary

DoD has made significant progress towards achieving more than awareness of the need to build the appropriate infrastructures, systems, and defensive posture to achieve the warfighter's vision of information superiority to support JV 2010. The Department is actively engaged in the planning, programming, budgeting, and execution of programs and resources that will prepare, shape, and respond to the future of warfare. The activities that occurred in 1999 are highlighted below and are described in detail in the following chapters of this report.

- DoD Public Key Infrastructure Policy

- DoD Computer Forensics Lab

- Computer Network Defense

- IA Vulnerability Alert

- Global Information Grid IA Guidance and Policy Memorandum

- Defense IA Red Teams

- Defense-Information Assurance Red Team Methodology

- IA Training and Certification

- Insider Threat Integrated Process Team

- IA Research

- Reserve Component Study

- Web Security Initiative

- IA Architectural Overlay

THIS PAGE INTENTIONALLY LEFT BLANK

2. Major Initiatives

2.1. DIAP Implementation

2.1.1. Objectives and Accomplishments

In a 30 January 1998 Memorandum, Dr. John Hamre, the Deputy Secretary of Defense (DEPSECDEF), directed the Defense-wide Information Assurance Program (DIAP) to be established under the oversight of the DoD CIO. DIAP would, therefore, form the core-organizing element for achieving a more comprehensive, coherent and consistent IA program. The Hamre memorandum directed the development of an Implementation Plan, and assigned responsibilities to the various Agencies and Office of the Secretary of Defense (OSD) offices to accomplish this activity.

DIAP began operation in June 1998 and continued to refine its organization and processes throughout 1999. In addition to finalizing the DIAP Implementation Plan and starting work on the DIAP Program Execution Plan, the DIAP team, in concert with Office of the Assistant Secretary of Defense (OASD) for Command, Control, Communications, and Intelligence (C3I)/CIO strategic planning efforts, made substantial progress with respect to strategic planning for the DIAP staff.

2.1.2. Implementation Plan

The DIAP Implementation Plan, signed by Mr. Art Money, ASD(C3I), on February 12, 1999, provides the management structure for the oversight and integration of all DoD IA-related programs. The document articulates the organizational responsibilities and relationships required to manage the DIAP as well as the internal structure and responsibilities of the DIAP staff.

The document also includes a description of the DIAP planning and programming development process, the DoD IA vision statement (as described in Section 2.1.4.2), and a charter for the DIAP Senior Steering Group. Roles and responsibilities include the following:

- **DoD Chief Information Officer (CIO).** The Department's implementation of the Clinger-Cohen Act assigns the DoD CIO responsibility for ensuring information technology (IT) and information resources are effectively managed to provide for the Department's operational requirements. DIAP is the mechanism to enable the DoD CIO to discharge his Defense-wide IA responsibilities.

- **DoD CIO Council.** The current charter for the DoD CIO Council mandates that the Council monitors and coordinates the Department's investment review, budget formulation, and financial execution processes for IT. Because the membership of the DoD CIO Council did not initially include some DoD components with significant IA responsibilities, DoD CIO Council has explored,

through the GIG activities, the expansion of the Council to ensure balanced representation across the Department.

- **National Manager**. The Director of the National Security Agency (DIRNSA) acts as the National Manager for National Security Telecommunications and Information Systems Security. He is directly responsible to the Secretary and Deputy Secretary of Defense for ensuring the security of all national security systems. In conjunction with the National Institute of Standards and Technology (NIST), DIRNSA provides Information Security (INFOSEC) technical guidance, advice and support to the U.S. Government Departments and Agencies. DIRNSA also acts as the U.S. Government focal point for cryptography and INFOSEC, and reviews and approves all standards, techniques, systems, and equipment related to the security of national security systems. DIRNSA assesses the overall security posture and vulnerability of national security systems and disseminates threat information related to its assessments. DIRNSA annually assesses the National Security Telecommunications and Information Systems Security Program budget recommendations of the Executive Departments and Agencies for the Executive Agent. The DIRNSA serves as an advisor to the DoD CIO on IA-related national security issues, consistent with the above authorities and responsibilities, and as a member of the Senior DIAP Steering Group.

- **Defense Information Infrastructure (DII) Advisor.** The Director, Defense Information Systems Agency (DISA), with management responsibilities for the DII, is responsible to the ASD(C3I) for the planning, development, and support of C3I systems that serve the needs of the National Command Authorities under all conditions of peace and war. Additionally, the Director, DISA, serves as the DII System Engineer and provides end-to-end system engineering and direction, including network management and security for the DII. Consistent with these responsibilities, the Director, DISA, serves as the DII Advisor to the DoD CIO, DoD CIO Council and the Senior DIAP Steering Group.

- **Senior DIAP Steering Group.** The original intent of the Implementation Plan was that the DoD CIO, Director, DISA, the Joint Staff (J6 – Command, Control, Communications and Computer Systems), DIRNSA, and Service command, control and communications and computers (C4) Chiefs would constitute the membership of a Senior DIAP Steering Group and would provide strategic direction and guidance to the DoD CIO and the DoD CIO Council on all IA issues. Subsequent to the signing of that document and upon review of the membership of the DIAP Steering Group, CIO Council and Military Communications Electronics Board (MCEB), the decision was made by ASD(C3I) to absorb the DIAP Steering Group into the existing organizations because the memberships of this steering group, CIO Council, and MCEB were virtually identical.

- **Director, Infrastructure and Information Assurance (formerly Director, Information Assurance).** The ASD(C3I) Director of Infrastructure and Information Assurance (I&IA) is the principal advocate for IA throughout the Department. The Director, I&IA, is responsible to the DoD CIO for the overall operation of the DIAP, and provides oversight to the DIAP Staff Director as

Executive Secretariat for the Senior DIAP Steering Group until that Group was absorbed into the CIO Council.

- **Information Assurance Group (IAG).** Originally, the Director, I&IA, was supported by the IAG, which served as the Department's principal IA forum. The IAG addressed a number of functional issues through a series of working groups composed of representatives from the Components. The principal responsibilities of the IAG Working Groups included establishing (1) Defense-wide functional objectives; (2) furthering their development, integration and coherent implementation; and (3) developing Defense-wide performance criteria. In February 1999, the IAG was realigned to provide support directly to DIAP. Subsequent to that change, and in an effort to reduce the duplication of panels, working groups etc., the decision was made in September 1999 to merge the IAG with the IA Panel of the MCEB because the two groups had nearly identical responsibilities and membership. That merger occurred in October 1999 with the first meeting of the combined groups. Further details of that merger and subsequent activities are provided later in section 2.4.4.2 of this report.

- **DIAP Staff Director.** The Staff Director is responsible for (1) coordinating DIAP development with the DoD Planning, Programming, and Budgeting System (PPBS); (2) developing a comprehensive process to assess the Department's return on its IA investments; and (3) providing for the continuous oversight of the execution of the Department's IA policies, functions and programs.

- **Intelligence Community (IC) Coordinator.** The IC Coordinator works to ensure integration and compatibility of IC and DoD IA efforts.

- **Joint Staff, Military Services, and Defense Agencies.** The Joint Staff, Military Services and Defense Agencies are responsible for planning and executing their IA responsibilities consistent with DoD policy and direction, their unique operational requirements, the DoD PPBS, and direction provided by the DoD CIO through DIAP.

2.1.3. Program Execution Plan

The organizational structure and business operations of DIAP have evolved over the last year to incorporate the experience of the DIAP staff in carrying out the assigned tasks. The Program Execution Plan (PEP), similar to a Concept of Operations, is being developed to provide detailed descriptions of the activities of DIAP and the interactions with the various organizations with which DIAP works. It will include Functional Mapping activities that define in detail what will be accomplished by each of the DIAP Functional areas. Additionally, the processes and relationships between DIAP and the PPBS will be articulated in the PEP. The document is currently in draft, with expected completion and issuance in the first quarter, CY2000.

One change is in the structure of DIAP staffing. Although not originally planned, the position of Deputy Director was added to address the number of administrative tasks required of any organization. Additionally, because of lack of available detail personnel from

the military Services and most of the DoD agencies, the liaison positions have been expanded to address coordination with those activities. The liaison position is the primary point-of-contact (POC) for DIAP with the Components and assists in identifying additional POCs within the parent component for special issues. Although not a formal part of the DIAP organization, functionally these liaison positions are critical to the successful achievement of the DIAP mission. The DIAP organization, modified as described, is illustrated in Figure 3.

Figure 3. DIAP Organization
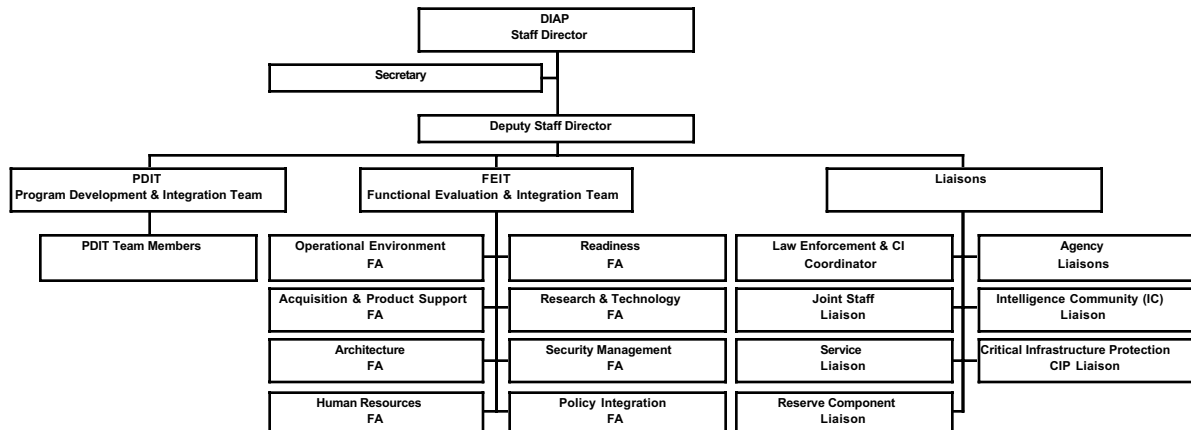
2.1.4. Strategic Plan

The DIAP staff is participating in a strategic planning initiative that began in September 1999 and will continue through January 2000. In this initiative, the DIAP mission, vision, guiding principals, and goals and objectives are being modified and/or developed which expand upon and carry out the goals and objectives laid out in the DoD IA Strategic Plan, as described previously in Section 1.2. Additionally, these goals and objectives expand upon the C3I goals and objectives, specifically Goal 2, "Implement Effective Programs for Establishing IA and Critical Infrastructure Protection (CIP)." The C3I goals and objectives and breakout for Goal 2 are provided in Annex 4 of this document. The tasks and subtasks within each objective, metrics and the Deployment Plan for the Strategic Plan will be finalized in early 2000.

2.1.4.1. DIAP Mission

The primary mission of DIAP is to ensure the Department of Defense's vital information resources are secured and protected by unifying/integrating IA activities to achieve information superiority

2.1.4.2. DIAP Vision

The DIAP vision statement provides that, by 2005, DIAP will be the model organization for implementation of enterprise-wide IA. This will be accomplished by performing the following:

- Institutionalizing IA in DoD mission areas and processes.

- Measuring and articulating improvements in the Department's IA posture.

- Identifying and justifying IA investments.

- Being recognized as a value-added partner within the IA community.

- Operationalizing IA to have situational awareness of the information environment.

- Being the primary resource for IA issues and concerns.

- Creating a National Passion for IA.

2.1.4.3. Goals and Objectives

The DIAP staff identified five goals and associated objectives to ensure the security and protection of the Department's vital information resources. The goals and objectives are as follows.

Goal 1:   Ensure a Comprehensive, Coherent IA Program Across the DoD.

- Objective 1.1.   Assess the state of DoD's IA posture.

- Objective 1.2. Ensure sufficient numbers of properly trained and certified IA professionals are available to accomplish the Department's IA mission.

- Objective 1.3. Ensure current and relevant IA policies, directives, and guidance are developed and implemented throughout DoD.

- Objective 1.4. Establish an integrated security management infrastructure (SMI).

- Objective 1.5. Understand and promulgate best practices in IA operational concepts.

- Objective 1.6. Be the advocate for IA research in the Department.

- Objective 1.7. Ensure that IA is an integral element/component of DoD Systems.

Goal 2:   Ensure sufficient DIAP resources to achieve the mission.

- Objective 2.1. Validate staffing requirements for DIAP.

- Objective 2.2. Establish additional permanent DoD billets for DIAP.

- Objective 2.3. Develop official Memoranda of Agreement to ensure that formal extendable tours are established for detailees to DIAP.

- Objective 2.4. Ensure that DIAP is manned by subject matter experts with established credibility, as determined by Objective 2.1.

- Objective 2.5. Ensure adequate facilities, equipment and connectivity to support the mission.

- Objective 2.6. Ensure that a defensible DIAP plan, program, and budget is inserted into the budgetary process.

Goal 3:   Ensure adequate IA resources are available throughout DoD.

- Objective 3.1. Develop a framework for an IA resource structure.

- Objective 3.2. Establish a program to identify IA in the PPBS FY2000.

- Objective 3.3. Review budget executions.

Goal 4:   Ensure awareness of DIAP throughout the DoD.

- Objective 4.1. Develop and maintain a comprehensive DIAP awareness program.

- Objective 4.2. Develop standard awareness products (e.g., (DIAP briefings, functional area briefings, programmatic briefing products, brochures, reports, etc.).

- Objective 4.3. Develop mechanisms for customer relationship management.

- Objective 4.4. Identify POCs from C/S/A for specific functional areas.

Goal 5:   Ensure integrated and coordinated interactions with agencies, departments, and components external to DoD.

- Objective 5.1. Integrate the Law Enforcement and Counterintelligence communities into DoD IA.

- Objective 5.2. Integrate IA issues with Critical Infrastructure Protection issues as appropriate.

- Objective 5.3. Coordinate with the Intelligence Community on appropriate IA-related issues.

2.2. Major Program Initiatives

In 1999, the Department initiated a number of major programs that will have significant improve the Department's IA posture. Some of the elements in these initiatives began in 1998, but it was in 1999 that significant progress was made. Other initiatives started this year will have a positive effect in future years. The following sections provide an overview of each of these initiatives. Key documents are listed in the Reference section of this report and can be made available for in-depth review upon request.

2.2.1. Public Key Infrastructure

The Department is taking major steps to reform its paper-based processes by transitioning to an environment of electronic information interchange. The DoD Public Key Infrastructure (PKI) enables the IA security services of data integrity, user-identification and authentication, user non-repudiation, and data confidentiality for electronic information interchange. This is accomplished by providing the public key (PK) technology-based keys, certificates, and associated management capabilities to support digital signature and encryption. These PK-enabled IA services and applications provide for the protection of transactions from unauthorized data disclosure and modification, and provide positive access control to system resources. To ensure interoperability among DoD users and to minimize operational costs, DoD will employ a PKI that is under a centralized management structure, yet will support outsourcing and distributed Service/Agency operation of some of the PKI components. The integrated enterprise-wide PKI will address a variety of security token technologies, support both commercial and federal standards, and meet overall DoD objectives for secure electronic transactions within DoD and the Federal Government, with our allies, and with elements of the private sector.

The DoD PKI is a critical underpinning of DoD's IA capabilities and its ability to achieve Information Superiority. A DoD-wide PKI enables the necessary IA security services for DoD leadership, warfighters, commanders, and support elements to make consistent risk management decisions in consideration of the highly interconnected, interdependent, shared risk environment in which daily operations are conducted. The PKI Implementation Plan for DoD, the DoD PKI Roadmap, the DoD X.509 Certificate Policy, and the DoD Certification Practice Statement are the guiding documents for establishing the enterprise-wide end-state for the DoD PKI and are described in the following sections. These documents also provide the foundation for the PKI strategy, and ensure that the Department is consistent in identifying PKI assurance levels commensurate with operational mission requirements and objectives, while maintaining compliance with applicable DoD policies.

2.2.1.1. DoD PKI Program Management Office

On April 9, 1999, Mr. Arthur Money, ASD(C3I) and DoD CIO, issued a memorandum assigning DoD PKI Program Management Office (PMO) responsibilities. National Security Agency (NSA) is the Program Manager and DISA is the Deputy Program Manager.

The DoD PKI PMO developed a PKI Implementation Plan for DoD (Version 2.0, dated 29 October 1999). The Implementation Plan documents DoD's detailed plan and timeline for the phased implementation of a DoD-wide PKI, and includes the framework and services

that provide for the generation, production, distribution, control, and accounting of PK certificates. This plan sets the course for DoD's realization of an integrated DoD-wide PKI service. It serves as the vehicle to coordinate PKI activities across DoD.

2.2.1.2. DoD PKI Policy

On May 6, 1999, Dr. John Hamre, Deputy Secretary of Defense, issued a formal DoD PKI policy. This policy emphasizes the importance of achieving Information Superiority in a highly interconnected, shared-risk environment by requiring that DoD IA capabilities address the diversity and pervasiveness of information, information systems, and infrastructures to support warfighting and business operations as part of DoD's GIG. The DiD uses a common, integrated DoD PKI to enable the requisite IA security services, and provides a solid foundation for DoD-wide IA capabilities.

This policy also seeks to maximize the use of commercial-off-the-shelf (COTS) technology to keep up with technology evolution and develop government-off-the-shelf (GOTS) solutions when necessary. The DoD PKI Policy establishes critical milestones in the evolution of the DoD PKI to aggressively implement a PKI that meets the requirements for all IA services, encourages widespread use of PK-enabled applications, and provides specific guidelines for applying PKI services throughout DoD. The DIAP is tasked to provide central oversight of all DoD PKI activities.

2.2.1.3. DoD PKI Front End Assessment

In conjunction with the DoD Program Review, as part of the PPBS, the DIAP participated in a DoD PKI Front End Assessment (FEA) to develop a consistent and coordinated baseline of the resources required for the implementation of the DoD PKI. Program Decision Memorandum (PDM) I, dated August 13, 1999, drew upon the findings of the DoD PKI FEA and the sequential IA program review of the DoD PKI. PDM I provided resources across the Future Years Defense Plan (FYDP) 01-05 to implement the DoD PKI.

2.2.1.4. PKI Roadmap for DoD

The PKI Roadmap for DoD establishes the enterprise-wide end-state target for the DoD PKI and outlines the DoD strategy and timeline for the availability of PKI capabilities. In addition, it assigns roles and responsibilities, and highlights critical issues and challenges that must be addressed in parallel with the implementation of this strategy. The Target DoD PKI shall:

- Provide an integrated PKI that supports a broad range of commercially-based, security-enabled applications, and that also provides secure interoperability within DoD and with its partners while minimizing overhead and impact on operations.

- Support certificate services that are standards-based, and support multiple applications and products, digital signature and key exchange applications, and key/data recovery. These certificate services would be commercially based (to allow for potential outsourcing, as appropriate), and would comply with the Federal Information Processing Standards.

- Employ centralized certificate management, decentralized registration, and use common processes and components to minimize the investment and manpower to manage and operate the PKI.

- Enable the associated IA security services at multiple levels of assurance as part of a comprehensive DiD.

2.2.1.5. DoD X.509 Certificate Policy

The DoD X.509 Certificate Policy (CP) is the unified policy under which a Certification Authority (CA) operated by a DoD Component is established and operates. A CA is an entity authorized to create, sign, and issue X.509 keys and certificates for public-key cryptography. It does not define a particular implementation of a PKI, nor the plans for future implementations or future CPs. It also does not define CP for CAs operated by external entities on behalf of DoD.

The CP defines the creation and management of Version 3 X.509 public key digital certificates for use in many information system applications that require communication between networked systems. Such applications include but are not limited to: electronic mail; transmission of unclassified and classified information; signature of electronic forms; contract submission signatures; and authentication of infrastructure components such as Web servers, firewalls, and directories. The network backbone for these security products may be unprotected networks such as the Internet or NIPRNET, or protected networks such as the SECRET Internet Protocol Router Network (SIPRNET).

2.2.1.6. DoD Certificate Practice Statement

The Certificate Practice Statement (CPS) identifies the implementation specific operational details of the DoD X509 Certificate Policy within a specified domain. It establishes the operating procedures for the CA and clarifies legal rights and obligations regarding the life cycle management of PK certificates. It defines the requirements and responsibilities of the Certification Management Authorities to include Certificate Authorities and Registration Authorities (RAs and local RAs (LRAs)). NSA will lead the update of the High Assurance CPS, the U.S. DoD Multilevel Information System Security Initiative Certificate Management Infrastructure (CMI), Information System Security Policy (ISSP) and CPS for Certificate Authorities, per NAG-69, NSA, October 1997, Fort Meade, Maryland.

2.2.1.7. Public Key Enabling of Applications

In accordance with the August 1999 PDM I, the Deputy Secretary of Defense directed the OASD(C3I), in coordination with the Director of Program Analysis and Evaluation (DPA&E), Joint Staff, Commanders in Chief (CINCs), Military Services, and the Directors of NSA, DISA, and DLA, to submit a policy for PK enabling of applications in accordance with the following schedule:

- By September 15, 1999, develop a draft policy and assign responsibility, as appropriate, for an integrated DoD-wide PK enabling of applications.

- By December 1, 1999, complete the policy and develop the criteria and framework for selecting applications to be PK enabled.

To take advantage of the IA security services that the DoD PKI provides, applications supporting electronic information interchange must be PK enabled. A PK Enabling of Applications Working Group was formed with representatives from all DoD components to address issues relating to this process. A draft policy was issued for coordination in late November 1999 that incorporates inputs from the working group. A software-based cost estimation tool is under development for use by all Components to assist in standardized cost estimations for the enabling of applications. The results of this working group, expected by the end of February 2000, may have a significant influence in budget decisions regarding the issues of enabling and costing applications for the PKI.

2.2.2. IA Training and Certification

The ASD(C3I) and the USD(P&R) jointly commissioned the IA and IT Human Resources Integrated Process Team (IPT) in September 1998. They charged the IPT to identify the critical IA and IT Management skill sets in DoD and to recommend mechanisms to promote the achievement and sustainability of those skills. Forty-five people from fifteen DoD Services and Agencies met beginning in late September 1998 to begin an intensive six-month analysis. Their goal was to recommend actions and policies that would lead to establishing a comprehensive and world-class human resources program for IA and IT Management within the Department. The IPT looked closely at the following areas:

- Taxonomy

- Occupational descriptions and career fields

- Certification standards

- Training program

- Accession and retention trends

The final report, entitled Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense, presents nineteen distinct recommendations to improve the way in which the Department manages its IT workforce.

Twelve of the nineteen recommendations directly affect IA training and certification. The IPT's most significant finding was that IA and IT Management personnel readiness is more problematic than simply providing training opportunities and financial/career incentives to IT professionals. Before those strategies can be attempted, the Department must learn the demographics of its IT population and know precisely what IT activities it is performing.

To address the issues identified in the report, the IPT recommended changes to the ways in which the Department manages its IT workforce. One recommendation takes the form of recognizing specific IA functions that reflect current duties of the information age. In addition, the IPT recommends coding the IT billets and all people who perform IT functions in a DoD personnel database so that career progression trends and training credits

can be tracked accurately. Finally, the IPT suggests linking standardized training and certification requirements to those coded billets and people so that no one with privileged access to information infrastructures is overlooked when it comes to critical IT preparatory and sustaining education.

The IPT report presents a strong case that the Department needs to take preliminary steps to substantially improve the way we manage our IA and IT workforce. The IPT concludes that in three to five years after these recommendations are fully implemented, the Department will have the personnel data needed to make proper decisions concerning the creation of a career management program for IT personnel. The report also includes an implementation timeline that recognizes the major steps to complete the recommendations and the schedule for doing so. The resources to implement these recommendations include significant time, personnel, and financial costs. However, the IPT is confident that the suggested course is a prudent one to position the Department appropriately to support the JV2010 concept of Information Superiority.

The report's recommendations and associated costs and timelines were briefed to the USD(P&R) and to the ASD(C3I). A briefing to the Deputy Secretary of Defense will be scheduled in early 2000, with approval to implement the many recommendations expected at that time. A detailed execution plan will be developed and monitored by the DIAP.

2.2.3. DoD Computer Forensics Lab

On September 24, 1999, DoD opened the doors to the DCFL. This is a state-of-the-art facility to process computer evidence in criminal, fraud, and counterintelligence investigations for the all of the Defense Criminal and Counterintelligence Investigative organizations. The Air Force Office of Special Investigations is the Executive Agent for DCFL. The DCFL currently has 42 positions for investigators and forensic technicians to process computer evidence as well as audio and video media in cases ranging from sexual child abuse to computer intrusions and espionage. DoD also convinced and provided funding for, the Federal Bureau of Investigation (FBI) to build a computer forensic capability that is co-located with the DCFL to build synergy with other criminal investigative organizations.

Already the DCFL has been instrumental in successful identification of computer hacking groups through computer media analysis. It has assisted in the neutralization of vulnerabilities in several high profile counterintelligence investigations related to national computer network defense activities including Solar Sunrise, Digital Demon, and Moonlight Maze.

2.2.3.1. Defense Computer Investigation Training Program

Also on September 24, 1999, the Defense Computer Investigation Training Program (DCITP) opened to provide computer investigative training for individuals and DoD elements to ensure defense information systems are secure from unauthorized use. DCITP coursework (in-house, on the road, and through computer-based training) offers more than nine courses, including System Administrator Incident Preparation and Response, Computer Search and Seizure, and Managing Computer and Network Investigations. The DCITP is co-located with the DCFL to help build a synergy for computer crime investigations.

2.2.4. Insider Threat Integrated Process Team

The ASD(C3I) established the IPT to foster the effective development of interdependent technical and procedural safeguards to reduce malicious behavior by insiders. The tasking required the IPT to recommend actions and policies leading to establishing comprehensive security, acquisition, and personnel practices to address the insider threat. The tasking described insiders as "individuals or organizational entities who have authorized physical or electronic access to DoD information and infrastructure resources." The term "threat" refers to the ability of such individuals or organizational entities to exceed or abuse their authorized access to such resources to exploit, attack, or otherwise adversely affect DoD information systems.

Stated more broadly, the objective of the Insider Threat IPT is to minimize the impact of the insider threat and, failing that, to minimize the potential damage inflicted on DoD information and information systems.

There are four basic sources of insider security problems:

- Maliciousness that results in compromise or destruction of information, or disruption of services to other insiders.

- Disdain of security practices that results in compromise or destruction of information, or disruption of services to other trusted operators. This problem results from willful:

  - public display of classified information; storage of classified material on unclassified media;

  - unauthorized destruction of classified or unclassified data (e.g., For Official Use Only information, personnel or payroll data, other records);

  - lack of classified material protection outside of controlled facilities, to include unattended laptop computers containing classified materials; and

  - disruption of systems regardless of the sensitivity of the information they contain.

- Carelessness in the use of an information system and/or the protection of DoD information. These problems are typically infractions of security policy and practices (e.g., breech of classified security requirements) for which the damage is usually determined to be minimal. While these insiders have the ability to exceed or abuse their authorized access to such resources, their motivation is not to exploit, attack or otherwise adversely affect DoD information systems.

- Ignorance of security policy, security practices, and information system use.

Although the focus of the IPT was directed to mitigating malicious insider activity, it is worth noting that improvements in the security environment not specifically directed at mitigating malicious insider activity may, in fact, mitigate the threat. For example, security improvements raise the security bar for everyone.

A wide range of choices is available to satisfy these requirements. Each choice brings with it a burden in human and fiscal resources and in implementation and maintenance time. For example, a number of different approaches, methods, and tools can be employed to define and enforce limits on overt access, to review recorded actions, and to detect unauthorized activity. Other requirements must be much more precisely articulated before technologists will be able to offer credible solutions. For example, while certain behaviors are obviously unauthorized, the precise distinctions between what is ethical, conformant to policy or legal, and what is unauthorized, is imprecise. To detect unauthorized activity the technologist first must have a precise and accepted definition of the term "unauthorized" and its constituent behaviors. In the most rigorous context, solutions to some requirements are currently beyond the state-of-the-art, such as non-refutable records of actions and detection of certain unauthorized activity. Research and development are needed to satisfactorily address these requirements. The risk model provides a way to begin to frame alternatives that can be applied commensurate with the criticality of assets, exploitable vulnerabilities and specific threats—balanced against the resources available and urgency to solve the problem.

Referring to the risk model, the Department must pursue the following strategy to minimize the impact of the insider threat. Failing that, the Department must minimize the potential damage to DoD information or information systems. These concepts are elements of an active security paradigm.

- Establish criticality. Determine what assets are critical to the mission; declare what must be protected and to what extent (DoD information and information systems), based on an analysis and assessment of what is required to accomplish the mission.

- Establish trustworthiness. Seek to reduce the threat by establishing a high level of assurance in the trustworthiness of people, practices, systems, and programs.

- Strengthen personnel security and management practices. Develop and support a motivated, skilled, and security-responsive workforce (deterrence).

- Protect information assets. Control asset sharing and isolate information and capabilities based on need-to-know (define and enforce limits on overt access and deterrence); identify and reduce known information system vulnerabilities; and employ state-of-the-practice and new technology to enforce and support security policies.

- Detect problems. Actively search for potential threats or problems whether isolated or correlated, that may result in anomalous or malicious activity (detection of unauthorized activity and deterrence).

- React/respond. Correct suspected and actual unacceptable insider behavior using sound personnel, personnel security and system management practices (mitigation of unauthorized activity)—and failing that, seek legal or other appropriate management remedies (response to unauthorized activity and deterrence).

In addition to pursuing this strategy, the Department also must refine and update policies, procedures, and practices to account for changes in operations attributable to changes in the

military mission, the changing international security environment, and advances in technology.

2.2.5. Computer Network Defense Working Group

In response to PDM I, August 16, 1998, the ASD(C3I), in coordination with the CINCs, Military Services, and Defense Agencies, conducted "…a comprehensive study to:

- Identify the core Computer Network Defense (CND) functions;

- Recommend an integrated, Defense-wide, enterprise CND policy and assignment of responsibilities;

- Develop a programmatic structure for CND to support preparation and review of the FY02-07 Program Objective Memoranda (POMs)."

To conduct a comprehensive study, the OASD(C3I) established a CND Working Group (CND WG) with representation from the Joint Staff, CINCS, Military Services, Defense Agencies, and Intelligence Community, and coordinated with related groups IPTs, i.e., the IA Enterprise Architecture Working Group, the ISSP, the Zero Base Review (ZBR) Working Group, and the Information Assurance and Information Technology Human Resources Integrated Process Team (IA/IT-HRIPT).

The CND WG used the Defensive Information Operations Front End Assessment (DIO FEA) Final Report as a baseline. Major contributions from the DIO FEA report included a Statement of Need, a preliminary set of core CND functions, and a federated architecture as the driving, principle for organizing and operating CND activities.

The CND WG identified the core functions of CND; developed a CND framework; and produced a draft DoD Directive for Computer Network Defense and POM Preparation Instructions for the FY02-07 PPBS Cycle. Additionally, the CND WG began development of an annotated outline for a DoD Instruction for Computer Network Defense, and coordinated with the Joint Staff regarding a proposed Chairman of the Joint Chiefs of Staff Instruction (CJCSI) for Computer Network Defense.

2.2.6. IA Research Activities

The major set of activities involving IA research revolved around the INFOSEC Research Council (IRC). The IRC coordinates, collaborates, and influences IA research within DoD (Defense Advanced Research Projects Agency, NSA, Army, Navy, and Air Force) as well as non-DoD Federal agencies (Department of Energy, NIST, Central Intelligence Agency, and others).

The activities the IRC conducted regarding IA include:

- Developing a "hard" problems list to help focus the community's IA research efforts, including topics such as:

  ❑ Intrusion/misuse detection and response

- Foreign and mobile code

- Controlled sharing of sensitive information

- Application security

- Denial of service

- Communications security

- Security management infrastructure

- Security in mobile environments

- Security engineering methodologies

- Influencing vendors

- Completing an IA research baseline/rollup that depicts "where is the DoD Community spending IA research dollars" to avoid duplication and identify potential areas for partnerships. The information in the database includes program name, funding organization, executing organization (which is often different from funding organization), funds involved, and other pertinent information.

- Sponsoring of "hot topics" in IA research to educate Senior DoD leadership on the status of the IA research and/or hard problems and their potential solutions. A sampling of these "hot topics" briefings include, malicious code, executable content, denial of service, and insider threat.

The IRC also surveyed commercial IA research at companies such as Lucent, IBM, Microsoft, and Intel. Contact was also made with the Security Research Alliance (SRA), a consortium of commercial companies working on security solutions, to ensure a DoD input into SRA activities. Follow-on activities in this area includes development of an IA Research Vision and Roadmap, as well as research gap analysis and metrics development.

2.2.7. Information Assurance Vulnerability Alert

Recent network assessments and external activities continue to demonstrate that widely known vulnerabilities exist throughout DoD networks, with the potential to severely degrade mission performance. The Department's increasing reliance on the accurate and timely exchange of information mandates that IA no longer be relegated to a secondary concern. IA is an essential element of operational readiness, and mitigation of IA vulnerabilities is a concern at the highest levels.

To protect DoD networks against potential vulnerabilities, there is an increased emphasis on the Information Assurance Vulnerability Alert (IAVA) process via the Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Information Assurance Vulnerability Alert (IAVA)," December 30, 1999. The initial requirement establishing this process occurred by DoD message to the Department in 1998. Implementation of the

requirements and responsibilities prescribed by the memorandum will ensure that Components take the required mitigating actions against new system vulnerabilities so that a serious compromise of DoD assets is avoided. A DoD Instruction formalizing the full IA vulnerability reporting and mitigation program is in development.

In 1999, DISA established a system for distributing vulnerability information to all DoD elements on behalf of OSD, issuing in the process 10 IAVAs (alerts), 3 IAVBs (bulletins) and 19 technical advisories. DISA also developed a database to immediately distribute vulnerability information to each system administrator, and to track and report on their response to these alerts. IAVA 2.0 enhancements include simpler/easier interface, secure automated upload of statistics, NIPRNET reporting on SIPRNET side if desired, DoD program fix action plans, DoD oversight reporting, reports for IAVA POCs, and DoD program manager acknowledgement.

The DISA-developed Vulnerability Compliance Tracking System (VCTS) has been briefed to the Navy, Air Force and U.S. Joint Forces Command (USJFCOM). The VCTS has been prototyped at U.S. Special Operations Command (USSOCOM), U.S. Space Command (USSPACECOM), and USJFCOM.

2.2.8. Reserve Components Study

The OASD for Reserve Affairs, Research, Training and Manpower (RA(RT&M)) chartered a study to take a look at Reserve Component participation in IA activities. The details of that study are described in the following sections.

2.2.8.1. Study Purpose, Scope, Methodology, and Organization

The principal purpose of this study was to identify opportunities for the RC of the U.S. military to perform IA missions in support of requirements that have been assigned to the DoD. As specified by the study sponsor, the DoD Critical Infrastructure Protection Plan (CIPP) occupied a central role in this study effort in that it served to establish the structural scope and to provide a technical framework within which IA functions could be defined. The RC study also addresses the related issue of recommending a direction to follow in the development of a database to catalog the civilian-acquired skills possessed by members of the RC, and it examines the relationship between IA and Weapons of Mass Destruction (WMD).

The RC study team developed an approach that began with the construction of a baseline assessment of current and projected RC capabilities performing IA activities as the foundation of the study effort. The capabilities baseline focused both on structural and organizational entities as IA capabilities, as well as intensely scrutinizing personnel skill sets to identify all possible personnel assets that might be able to contribute to the performance of IA missions or IA-related tasks. A parallel effort was undertaken to capture the specific IA tasks assigned to DoD. This process consisted of an intensive review of national, departmental, Joint Staff, Agency and Service statutes, regulations, directives, policies, and procedures to identify the types of IA functions DoD was charged to accomplish. To exploit the leads developed by the literature review, and to capture the ground truth from personnel actually executing IA missions and tasks, the study team conducted an extensive visit program to more than 50 commands, staffs and agencies with direct responsibility for

IA. Using the results of the document review and staff visits, the study team developed recommendations for specific actions that ASD(RA) could pursue in which the RC could make positive and immediate contributions to the IA posture of the DoD.

The study was organized into five tasks that are summarized below.

- Task I dealt with the construction of the RC IA Capabilities baseline identifying RC organizations and elements and providing personnel inventories based on IA skill sets outlining the resources available to each RC to perform IA missions and tasks.

- Task II provides a listing of IA requirements for which DoD and its Components have responsibility within the department and to national level entities.

- Task III presents the study team's recommended opportunities for employing the RC capabilities identified in Task I to support to the IA missions identified for DoD in Task II and addresses the issue of cataloging of civilian-acquired skills.

- Task IV delivers the study team's assessment of the relationship between IA and Weapons of Mass Destruction as presented to the Special Assistant to the Secretary of Defense for Military Assistance to Civil Authorities.

- Task V provides the composition and results of the Senior Review Panel's consideration of the final study results, which took place on November 30, 1999.

2.2.8.2. Study Recommendations and Findings

- **Comprehensive RC IA Architecture**: Recommend undertaking a follow-on study effort by the Services and Agencies, under DoD auspices, to develop an IA Master Plan that includes and integrates the significant capabilities and resources of the Reserve Components into a comprehensive Total Force IA architecture.

- **Capabilities and Requirements Clearinghouse**: Recommend that ASD(RA) support the establishment of an OSD or Joint Staff element to serve as a clearinghouse to match RC capabilities and requirements in support of DoD IA missions.

- **Civilian-Acquired Skills Database**: Recommend the ASD(C3I) Defense Planning Support System (DPSS) database as the best option for further development and adaptation as the primary vehicle for cataloging civilian-acquired skills of RC. Acceptance of this recommendation must be accompanied by directives which make registration and completion of the individual skills online data form mandatory for all RC personnel and that a promotional effort be undertaken by ASD(C3I) to more fully explain the emerging DPSS.

- **RC Augmentation to the JIOC**: Recommend a comprehensive study effort be launched in conjunction with the Joint Information Operations Center (JIOC) and USSPACECOM to establish the type and level of RC support that could be provided to assist the JIOC in the accomplishment of its tasked missions.

- **Website Review**: Recommend that RC support to the Joint Website Risk Assessment Cell (JWRAC) be increased, and that similar RC elements be formed to expand the DoD Website Review Program through the adoption of virtual operations from centralized unit drilling locations or RC member residences.

- **IAVA Compliance**: The development of IAVA compliance as a RC mission represents an area where the RC is exceptionally well suited and positioned to assist DoD in meeting a requirement not comprehensively addressed with current resources. The potential exists to use this mission as the basis around which to organize RC elements specifically tasked to perform IAVA compliance validation missions.

- **Education and Training Packages Description**: Recommend the expansion and further development of efforts such as those underway at the Vermont Army National Guard to construct exportable IA education and training packages in support of the DoD overall IT personnel training mission.

- **Professional Accession and Sustainment**: An area the study team considers essential involves the implementation, or at least further consideration, of several personnel management measures necessary to facilitate accession and address sustainment of IT professionals in the RC force. Without some adjustments and accommodation in the personnel management area, both the Active Component and Reserve Component will have difficulty attracting and retaining the IT professionals needed to fulfill IA missions within the DoD.

- **Legal Issues Symposium Description**: Recommend ASD(C3I) convene a "Legal Issues Symposium" to identify, illuminate and discuss the full range of legal, regulatory and policy issues that affect the performance of IA, IO, and Intelligence Support to IA/IO activities by the RC as part of the Total Force.

- **Vulnerability Assessment Training**: Recommend the RC take on the task of developing a Vulnerability Assessment Training course for use throughout DoD.

- **Missions for Joint Virtual Units**: The study team identified and recommends the following types of IA and IA-related mission areas that are appropriate for future Joint Virtual Units:

  - Website review

  - Computer Network Defense/Exploitation support

  - IAVA compliance

  - Baseline intelligence analysis and support

  - "Blue Teaming" Vulnerability assessments

  - Incident response

  - Education and training

- Exercise support

- Support to agencies/elements external to DoD

- Critical Infrastructure Mapping

- **Reimbursable Funding Authority for IA**: Recommend that ASD(RA) seek Congressional language authorizing a Reimbursable Funding Authority for RC Information Assurance/Information Operations activities in support of DoD missions similar to that currently authorized for RC intelligence support activities.

- **Intelligence Support**: Recommend that the ASD(RA), in conjunction with ASD(C3I), commission a follow on study to lay out a comprehensive plan for the refocused utilization of RC intelligence capabilities to support DoD IA operations. The study should specifically address the following areas:

  - Use of RC intelligence assets to support predictive intelligence.

  - Development of IO JRICs as intelligence support of IA Centers of Excellence.

  - The conduct of Open Source Intelligence Operations from virtual locations to include "home drilling".

  - The applicability of the "NSA Model" to the conduct of RC intelligence support of IA operations.

  - Support of existing RC IA initiatives with existing RC intelligence capabilities.

  - Use of RC intelligence assets to support Unified Command's MDCI efforts.

- **Critical Infrastructure Mapping**: Recommend that the RC augment the Navy's Joint Program Office - Special Technology Countermeasures to enable them to conduct mapping and modeling of Critical Infrastructure.

- **CIPIS Augmentation**: Recommend the Critical Infrastructure Protection Integration Staff (CIPIS) be augmented by RC personnel who by reason of civilian acquired expertise are able to effectively liaison in CIPP sector areas.

- **Joint Task Force-Computer Network Defense (JTF-CND) Augmentation**: Recommend the ASD(RA) actively support the USSPACECOM efforts to secure 30 additional RC billets for JTF-CND in order to provide the JTF-CND with a capability to conduct continuous, sustained, full spectrum CND operations.

- **Weapons of Mass Destruction (WMD) and IA**: The study team found no direct or unique relationship between WMD and IA. By definition, WMD are employed to directly inflict a maximum number of casualties or as an adjunct to catastrophic destruction of facilities through the detonation or distribution of explosive, incendiary, chemical, biological, or nuclear material. By definition, IA

protects and defends information and information systems. The target of WMD is people not information or information systems. It is expected that a cyber attack may well be planned to multiply the disruptive or terror quotient of WMD employment, or to retard consequence management actions by responding emergency services. However, the techniques, tools and avenues of attack in this instance would be the same as those anticipated in any other cyber attack. There is nothing unique about the risk mitigation, detection, reaction, response and restoration functions of IA when it is associated with a WMD event.

2.2.9. Global Information Grid IA Guidance and Policy Memorandum

In December 1998, the DoD CIO launched the Global Networked Information Enterprise (GNIE) initiative. This initiative, subsequently renamed Global Information Grid (GIG), covers all the major aspects of IT including computing, communications/networks, interoperability, technology, and resources, as well as IA. The goal was to develop fully coordinated policies, architectures, and resources implementing programs that will better align enterprise-level communications and information processing, security, operating procedures and technology initiatives across the Department. The proposed GIG IA G&PM addresses not only confidentiality of the Department's information, but also its availability, integrity, and the need for strong identification and non-repudiation services. It incorporates the Defense-in-Depth strategy described in last year's annual report, and establishes a closer working relationship with the intelligence community. All of the GIG policies will first be issued as DoD CIO G&PM, and then transition to formal Department-level Directives and Instructions.

2.2.10. Web Security Initiative

This initiative improves the Department's overall security posture by sensitizing DoD personnel to the adversarial value of unclassified information and the need to balance risks when electronically publishing to unclassified websites otherwise innocuous information. The Worldwide Web provides the DoD with a powerful tool to convey information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies, and programs. Web technology is at the heart of the Defense Reform Initiative and is key to the reengineering and streamlining of our business practices. Similarly, fundamental to the American democratic process is the right of our citizens to know what government is doing, and the corresponding ability to judge its performance. However, the Web can provide our adversaries with a potent instrument to obtain, correlate and evaluate an unprecedented volume of aggregated information regarding DoD capabilities, infrastructure, personnel and operational procedures. Such information, especially when combined with information from other sources, increases the vulnerability of DoD systems and may endanger DoD personnel and their families.

All DoD Components that establish publicly accessible websites are responsible for ensuring information that is published on those sites does not compromise national security or place DoD personnel at risk. By authorizing the establishment of websites, Component heads assume a management responsibility that extends beyond general public affairs considerations regarding the release of information, into the realm of operational security and force protection. Component heads are responsible for enforcing the application of comprehensive risk management procedures to ensure that the considerable mission

benefits gained by using the Web are carefully balanced against the potential security and privacy risks created by having aggregated DoD information more readily accessible to a worldwide audience.

In view of the growing information role of the Web within DoD, on September 24, 1998, the Deputy Secretary of Defense issued guidance addressing these vulnerabilities and directing several actions. Actions included the immediate removal of specified types of sensitive information from all DoD web pages, use of Reserve Component assets to conduct on-going operational security and threat assessments of Components' Websites, and development of additional policy and procedural guidance.

Subsequently, on December 7, 1998, the "Website Administration Policies and Procedures" were issued. Those policies and procedures are currently being staffed for inclusion in the formal DoD publication system as a DoD Directive and Manual. To mitigate the vulnerabilities, the policy:

- Requires all unclassified information be reviewed prior to its being placed on DoD websites

- Provided guidance on the types of information that should not be posted on publicly accessible websites

- Identifies processes for determining vulnerabilities and provides guidance on the protection afforded by various types of security and access controls

- Directed comprehensive, multi-disciplinary security assessments of DoD websites be conducted and established an annual requirement for continuance of such assessments

To provide the on-going operations security and threat assessments of publicly accessible component websites, the Deputy Secretary of Defense approved the Concept of Operations for the JWRAC on February 12, 1999. The JWRAC, staffed by a cadre of 22 service members from the Reserve Components, began operation on March 1. In execution of its mission, particular attention will be given to cross sectional analyses of DoD web information, to trend analysis and to data aggregation. During its first six months of operation, the JWRAC identified nearly 800 instances of potential policy violations which were forwarded to the appropriate offices for correction.

While the policy requirements and the JWRAC assessments have made a measurable difference, more remains to be done. Actions are underway to standardize website privacy and security notice warning banners, to develop policy on the use of mobile code to decrease the risks associated with malicious executable content, and to address the need for improved awareness of website administration and Operations Security (OPSEC) considerations through appropriate training courses and participation in conferences. Significant among the training efforts are the Web Security course developed and taught by the Interagency OPSEC Support Staff, and the planned inclusion of an OPSEC module in the four basic Public Affairs courses taught at the Defense Information School, which should be available by February 2000.

Although significant strides have been made to improve the security of the DoD Worldwide Web presence, continuing effort will be required to ensure the appropriate balance between security and privacy and the use of the web as a critical business tool for the Department.

2.2.11. Defense-Information Assurance Red Team Methodology

To gauge the state of operational readiness, periodic assessments of the operational processes, systems, and organizations are performed. The DIAP calls for an effective process for routinely assessing the operational readiness of the Department's information systems and networks. Such independent assessments, known as red team activities, provide an impartial perspective on the vulnerabilities that could be exploited by an adversary. IA red team activities are defined as:

> "An independent and threat-based effort by an interdisciplinary, simulated opposing force, which, after proper safeguards are established, uses both active and passive capabilities on a formal, time-bounded tasking to expose and exploit IA vulnerabilities of friendly forces as a means to improve the readiness of DoD Components."[10]

As such, IA red team activities are not limited to computer network attacks; red teams also employ physical, social engineering, operational security, or other types of attacks. While red teams are by definition exploitative, they can support a wide range of approaches, from covert, no-notice, red team activities to overt training-oriented red team activities, and can be broadly applied (e.g., DoD-wide red team activities) or used in small-scale applications (e.g., embedded system testing).

While many DoD organizations have embraced the concept of red teaming and have taken steps to implement red team activities into their security assessments, there has been no standardization in red team methodology across the Department. For example, the definition of red teaming to Organization "A" may be totally different than to Organization "B". Consequently, it is difficult to measure our readiness or have confidence in our ability to deter an adversary from exploiting our vulnerabilities.

In an attempt to introduce standardization to the IA red teaming process, the OASD(C3I) developed an IA red team methodology through a collaborative effort involving many of the red team organizations within the IA community.

The Defense-Information Assurance Red Team Methodology (D-IART), focuses on DoD requirements, and a companion Information Assurance Red Team Handbook is suitable for use throughout the Government. Both the D-IART and the Handbook provide a methodology for designing, developing, assembling, and conducting red team activities. By documenting a well-defined and repeatable process that captures the insights and expertise of government and industry organizations that perform red team activities, the D-IART strives to ensure all DoD red team activities have a consistency of purpose, a commonality of structure, and meaningful and comparable results. It is intended to aid in the selection, design, assembly, and conduct of red team activities across the broad spectrum of attack

---

[10] Footnote source.

types and intended operational impacts. The methodology outlined in the D-IART is intended for both singularly focused attacks and attacks across the full spectrum of IA, to include physical, psychological, and system attacks. The methodology also is intended to address a range of targets, from limited scope and single function targets to broad-ranging targets that influence worldwide U.S. military operations. The methodology is intended to be flexible enough to accommodate limited impact attacks, such as notional attacks, and fully functional attacks on operational systems.

The D-IART and Handbook define the activities associated with the four phases of red teaming: Pre-Planning, Planning, Attack, and Post-Attack. In the pre-planning stage, the objectives of the red team are determined in conjunction with the goals of the larger activity. In the planning phase, specific targets, attack mechanisms, and resources are selected, legal review is performed, and permissions are acquired. In the attack phase, the activity is conducted; and in the post-attack phase, results are accumulated, analyzed, interpreted, and disseminated. Both the D-IART and Handbook are available in a CD-ROM which provides a Red Team tutorial, as well as the copies of the "written" documentation.

2.2.12. IA Architectural Overlay

The Department has significant concerns at the enterprise level regarding attaining sufficient protection for its myriad of C/S/A information systems. At the enterprise level, these systems become a "system of systems" with fixed and dynamic information connections interlaced among the C/S/As to form a highly complex web of information exchanges. Achieving affordable systems that meet various mission needs and are appropriately protected in this shared risk environment is an extremely difficult and complex task. Compounding this problem is the evolution of existing applications to make them more integrated, more distributed, and more widely interconnected.

OSD(C3I) convened a small, but representative, quick-reaction IA Architectural Working Group to assemble a recommended course-of-action and a detailed plan of execution to:

- Develop preliminary IA Architectural Concept(s) for all standard views

- Utilize Communications and Communication Information Architecture, Joint Task Force - Noncombatant Evacuation Operation Scenario for a starting point upon which to build IA architectural products (Operational, Systems, Technical)

- Provide minimal (AS-IS), preferred (TO-BE), and unconstrained (GOAL) recommendations (with staff and resource estimates) to include preliminary architectural concepts, examples, and guidance.

The effort is underway and expects to deliver its products (reports, Information Exchange Requirements (IERs), and architectural documents according to C4ISR Framework guidelines throughout FY 2000.

Organizations involved in the working group are Joint Staff: ASD(C3I)/(I&IA); the DIAP; J6K; DISA, NSA; U.S. Central Command (USCENTCOM); U.S. Pacific Command (USPACOM); MITRE; IDA; and several Contractors: BETAC Corp (now ACS Defense), Booz-Allen-Hamilton Corp.

An architecture is an abstraction (or set of abstractions) that provides the means to describe and think about something within a general or specific context (perspective) before building it, while building it, and after it is built. Architectures allow the expression of concepts, principles, structural forms, functions, and attribute properties through the use of specific views reflecting the possibilities, desires, goals, constraints, and feasibility trade-offs from varying perspectives. Views may have overlays that provide unique focus to a perspective or concern within a view or across one or more views.

The central data repository for this IA Overlay is the Joint C4ISR Architecture Planning/Analysis System (JCAPS). The data will be accessible through the SIPRNET. JCAPS will also be the principal tool used in the continued development of IA Overlays to support other architectural efforts such as the Joint Operational Architecture. Other tools may continue to be used in the development of the IA Overlays as long as the data can be transferred to the JCAPS database.

The DoD Enterprise IA Architectural Overlay Set is an information "instrument" comprised of a set of living documents that are constantly under revision. This "document" includes Operational, System, and Technical subsets and incorporates or reflects other supporting documentation such as the Information Assurance Technical Framework (IATF), the Defense Goal Security Architecture, and the Defense Advanced Research Projects Agency's (DARPA's) Advanced Information Technology Systems Reference Architecture.

2.3.   Intelligence Community Cooperation

DoD and the IC CIO office have continued the coordination efforts begun in the previous year. There have been a number of activities where coordinated effort has been critical. These are as follows:

- **IA Policy Board (IC IAPB).** The IAPB serves as the Intelligence community's principal information assurance forum to coordinate and formulate community level information assurance policy that impacts areas affecting the security and/or interoperability of multiple IC members.

The IAPB is responsible for developing community-wide IA policies, strategies, and technologies to mitigate information systems vulnerabilities, formulating a comprehensive information systems/information assurance architecture that supports interoperability of multiple Intelligence Community members, and identifying and recommending actions to eliminate gaps and shortfalls in IC IA activities and programs. The IAPB met on a bi-weekly basis throughout the year to work/discuss/resolve a number of issues on behalf of the IC CIO. Most time consuming was the development of a PKI policy for the IC and the corresponding Certificate Practice Statement. Other issues included: development of a policy to protect email on unclassified networks; review of DoD's Global Network Information Enterprise IA policies; coordination of the Intelligence Program Decision Memorandum (IPDM) with respect to IA programs/issues; along with the DoD completed a Congressionally directed action to provide the Senate Select Committee on Intelligence an assessment of the policies, procedures, and technologies implemented by the various Intelligence Agencies and Offices to secure/protect their computer and telecommunications systems; development of an IC Asynchronous Transfer Mode (ATM) Security Policy; identification of IA/IT training needs for the IC; a working group to review policy for

second party dissemination; and review/coordination of a Top Secret and Below Initiative (T-SABI). The IAPB also received a number of technical/research and development IA initiative briefings from both government and industry representatives throughout the year.

- **Top Secret/SCI and Below Initiative (T-SABI).** To support current and future critical operational missions and to facilitate information transfer, sharing, and collaboration, the Intelligence Community requires the connection of Top Secret/Sensitive Compartmented Information (SCI) systems to information systems with different security domains (e.g., different/lower classifications, compartments, or releasability). The community-developed T-SABI policy defines the interconnection process and procedures to ensure that all T-SABI connections are implemented and protected in accordance with the requirements of Director of Central Intelligence Directive 6/3 and establishes community-wide standard processes to certify and accredit new T-SABI connections. In February 1999, NSA presented the T-SABI initiative to the Defense and Intelligence Community Accreditation Support Team (DICAST) to demonstrate the need for T-SABI and to provide an approach for using the existing DoD Secret and Below Interoperability (SABI) process to meet the T-SABI objectives. The two main points were (1) that more than 30 different types of security guards are currently in use, many of which do not have current documentation or accreditation and (2) several hundred SCI-to-collateral interfaces were identified. A T-SABI policy was subsequently developed and coordinated within the DoD and IC. The final draft is being prepared for consideration by the IC Information Assurance Policy Board (IAPB). Upon IAPB approval it will be submitted to the IC CIO Executive Council for approval as an IC CIO Policy

- **IC PKI Policy (IC PKI).** There is an increasing requirement for affordable interoperability for secure communications and collaboration between members of the IC. A critical foundation for achieving this requirement is the establishment of a general-purpose PKI that supports a broad range of applications on the SCI networks that are the backbone for IC communications. The IC PKI will provide IC member organizations strong identification and authentication, data integrity, digital signature, and encryption services for all information system-based communications and services traversing community SCI networks.

- **IC Privileged User Panel.** The Director of Central Intelligence (DCI) requested the Intelligence Community (IC) develop a monitoring and adjudication program for privileged users. A Privileged Users Panel was created to address this objective and met for the first time on December 10, 1999, chaired by Defense Intelligence Agency. It is estimated that 10% of the IC work force may be in the privileged user category. The numbers of systems administrators, software developers, and local area network (LAN) support personnel reflect the increased reliance on technology. This is a huge vulnerability when compared to the small number of crypto-communicators who operated communications units in the past. IC participants noted that their polygraph examinations provide an increasing number of leads to people who exercise poor security with their agency's automated systems.

- **IC Second Party Working Group.** The DIAP participated in an IC working group trying to identify and, if necessary, recommend changes in IC component policy governing access to U.S. information systems by foreign nationals. The group is chaired by Mr. William Dawson, Deputy of IA in the IC's CIO staff. The group is also looking

at access to U.S. information through foreign networks. They want to develop a community process for maintaining and revising these policies for future community use. Since they haven't restricted themselves to SCI information only, it is important for OASD (C3I) to follow their activities and bring DoD's efforts and policies to the table.

- **DICAST.** The DICAST was established by the Intelligence Systems Secretariat under the authority of Community Management Staff (CMS) letter 97-00176 as a permanent subgroup to the Senior Information Managers (SIM) Panel. The purpose of the DICAST is to facilitate the joint management of risk brought about by interconnecting the networks of the DoD and Intelligence Community Components (e.g., member Agencies, Joint elements, Community Staff). DoD members include the Services, Defense Intelligence Agency (DIA), NSA, DISA, National Imagery and Mapping Agency (NIMA), National Reconnaissance Office (NRO), JS and OASD(C3I). The DICAST is chaired by Mr. Paul Livingston, Intelink Management Office.

2.4. DoD Components

2.4.1. Department of the Army

In response to Deputy Secretary of Defense directives, the Army has made substantial progress in formulating and implementing IA initiatives and has accelerated implementation of its Network Security Improvement Program (NSIP) by over two years. The NSIP is a three part approach that emphasizes:

- Policies and Procedures - Establishing policies, tactics, techniques, and procedures (TTP) to secure tactical and sustaining base information systems across the full spectrum of conflict.

- Technology Insertion - Integrating state-of-the-art hardware and software security solutions into both the sustaining base and battlefield/digitized force C4I operational, systems, and technical architectures.

- Training - Identifying training and retention requirements and providing training opportunities.

Major Army achievements and initiatives consist of:

- Establishing a "Perimeter Defense" around all Army networks and systems by deploying firewall and firewall-like technologies and intrusion detection system (IDS) monitoring at all of the Army's NIPRNET gateways (currently 158), monitoring 458 critical Army servers with IDS, and instituting 24x7 monitoring of all Army networks.

- Launching a vanguard Army Biometrics Information Technology and IA Initiative to formulate policy for the acquisition, testing and evaluation, and use of biometrics products to improve the methods and technologies used to grant access to Army information and information-based (e.g., weapons) systems. The Army is conducting a Congressionally-sponsored proof of concept to replace passwords with biometrics applications in both sustaining base and command

and control (C2) tactical operations center environments. Initial results will be reported in the first quarter of Fiscal Year (FY) 2000.

- Implementing a DiD strategy that incorporates both technical and non-technical solutions, employing multiple protections at different layers throughout the information systems and network infrastructure, to include:

  □ Developing a modem dial-in (login and password authentication) security policy that was adopted by the Office of the Secretary of Defense (OSD) DoD minimum security guidelines.

  □ Identifying, and eliminating or securing, back doors into Army systems and networks, to include unsecured NIPRNET, internet service provider, point-to-point, and dial-in connections and other unsecured connections from activities like the Defense Research and Engineering Network and the Tri-Service Infrastructure Management Program Office. This is being accomplished in accordance with OSD policies and minimum security guidelines.

  □ Centrally purchasing and deploying over 2,270 network and host-based IDS and 670 firewalls to reinforce/increase the hardening of firewall/firewall-like technology and IDS infrastructures fielded by Army Major Commands.

  □ Installing proxy cache engines at select locations to protect publicly accessible web servers, facilitate registration and oversight of Army websites, and to proxy access to other protocols and services.

  □ Reengineering the Army Domain Name Service (DNS) infrastructure to maintain anonymity of the Army DNS system by rewriting lower tier server records to prevent additional DNS information from being accessed.

  □ Mandating that an installation's information infrastructure architectures for all Army posts, camps, and stations include an approved systems and network "security stack."

- Expanding and enhancing the types and numbers of training opportunities available to Army IT specialists, to include:

  □ 2760 military, civilian, and support contractor system administrators and network managers are trained annually at 11 resident "school house" sites in the continental United States (CONUS), the Pacific, Korea, and Germany.

  □ 800 IT personnel attend quarterly IA workshops conducted worldwide.

  □ 600 IA Officers are trained annually by mobile training teams deployed worldwide.

  □ 300 Army military, civilians, and support contractor IT personnel are trained annually at Ft. Huachuca, Arizona in IDS and firewall employment.

- Licensing of over 800 computer based training courses for use by military and civilian personnel.

- Initiating an Army Vice Chief of Staff-directed Army-wide IT/IA workforce study to comprehensively review recruitment, retention, education, training, certification, and career fields for Army IT/IA personnel. Findings and recommendations will be reported in phases from April through August 2000.

- Standing up an Army Compliance Verification Team to conduct Army-wide random checks to confirm that OSD and Army-mandated security procedures and fixes have been implemented.

- Planning and programming support requirements to field Class 3 Medium Assurance PKI to Army posts, camps, and stations in FY 2000, to provide all active Army military and civilian personnel with Class 3 identity certificates by October 2001, and to evolve to higher assurance Class 4 certificates hosted on smart cards as standards and technology mature.

- Application of IA policies, TTP, and training requirements and insertion of IA technologies/tools into the tactical force - First Digitized Division (FDD), to include:

  - Implementation of certification and accreditation requirements for all FDD systems, to include weapons systems.

  - Revision of the Army Protection Plan to integrate information systems protection into battlefield information systems, networks, and network infrastructure.

  - Employment of vulnerability assessments, red teaming, and information operation assessments to FDD systems and networks.

The Department of the Army's goal is to achieve a seamless IA environment from the sustaining base to deployed/digitized forces across the full spectrum of operations.

2.4.2. Department of the Navy

The Navy's efforts to achieve IA continues to capitalize on successful programs like Information Technology for the Twenty-first Century and the Navy / Marine Corps Intranet programs. The Navy is applying numerous protections to safeguard Department of the Navy (DoN) information and information resources. Most notable is the DiD security strategy, which will mitigate the Navy's and Marine Corps' formidable risks associated with network operations and knowledge-centric warfare. No protective measures provide for perfect or absolute security. Therefore, to protect the DoN network enterprises based on the DoD concept, the Navy has applied several network security appliances and technologies in combination. Ongoing DoN IA activities include:

- Continued implementation and use of firewalls to provide overall perimeter security. This is our front door for connections to the public networks. While firewall technology continues to improve, it alone does not provide complete

security. Therefore, the Navy will continue to use firewalls in conjunction with other devices.

- Focus on IDS technology. IDS continues to improve as the Navy's investment increases. But, like firewalls, this tool cannot be relied on by itself. IDSs have great utility but accurate attack assessments in near real-time is a serious deficiency. Intrusion detection technology will continue to be a high focus area for the next five to ten years.

- Support for PKI. PKI will be aggressively pursued to achieve increased security in identification and authentication, integrity, non-repudiation and confidentiality, constrained only by current technology and financial resources. Because of its immense promise, PKI is a major Navy and Marine Corp IA priority.

- Introduction of Key Management Infrastructure (KMI). The introduction of PKI technology and its associated CMI, will establish several unique and independent key and certificate infrastructures. Maintaining separate infrastructures is neither cost- nor manpower-effective. Consequently, the Navy is supporting a new initiative, jointly undertaken by DoD, with NSA as lead, to introduce a KMI that will be the framework for a single integrated key and certificate management solution for all classification levels.

- Participation in IA working groups. Participated in the DoD PKI Working Group, Deputy DoN CIO participates in the DoD PKI Senior Steering Committee, member of the DoD Information Security Systems Program Zero Based Review of funding requirements for information systems, DoN/CIO was appointed by the DoD PKI PMO to chair a committee to produce the Target Token Strategy for the DoD, Developed and wrote the DoN PKI Implementation Plan, established/monitored PKI pilots and projects.

- Participation in IA implementations. Participated in implementation of the DoD PKI, including the DoD PKI Front End Assessment initiative and PKI budget/funding discussions, DoD PKI PMO planning meetings, working group efforts (i.e., the Joint Key Management Infrastructure Working Group and the Certificate Policy Management Working Group, and hosted a PKI Implementation Planning Conference for Navy and Marine Corps second echelon commanders, commenced development of DoN PKI Implementation Plan.

- Support for Smart Card. The Department of the Navy is aggressively pursuing the cryptographic Smart Card.

- Support for multilevel security solutions. The Navy continues to pursue new and improved solutions for Multilevel Security, Multiple Security Levels and Coalition/Allied Interoperability. Although great progress has been made through the SABI initiative, this initiative continues to fall short of meeting the warfighter's requirements.

- Long term security training. In addition to the security systems being pursued above, the DoN is making the commitment and investment for near and long term solutions to security needs of training and engineering. Unfortunately, due to the dynamic nature of the IA program, some of the unfunded mandates and requirements of today are at the expense of future requirement initiatives.

- Recruitment, retention, education and training of Naval/Marine personnel engaged in IA are prerequisites to operational readiness and success during peacetime and conflict. Introduction of new networking technology and the introduction of new organizations with new missions also introduces new education and training requirements and challenges. This new mission will place the Navy in the forefront of defining new core skills associated with CND, developing associated education and training requirements, and integrating these skills with attack and exploit disciplines.

- IA awareness has improved tremendously throughout the Navy and DoD in the last two years, and progress continues. Due to the increase in the visibility of the program initiatives, new requirements continue to evolve as new systems continue to develop, integrate, and technology and policy evolve. It is imperative that IA administrators, professionals, and consultants stay current with the trends in the technology. Personnel resources for quality control of implementations continues to be an issue as industry increasingly become aware of their problems and the promising profit margin of this area. The commercial sector's continuing trend to leverage DoD investments in research, development, and resources will be at the cost of qualified and quality people from within DoD.

- Research and Development efforts will be a continuation of current initiatives to design, develop, and evaluate security solutions for DoN operational elements. We plan to include product assessments, tailored and developed standards, processes, and tools for Navy-unique applications. The security investments will also support integration of new capabilities and products to better secure Navy information systems and networks.

- Procurement efforts will be a continuous effort to procure, test, integrate and install high grade security products to satisfy Chief of Naval Operations (CNO) validated requirements. Procurement requirements are expected to increase due to rapid pace of technology advances and the continual need to replace, upgrade, and refresh technology within security product lines. Rapid production of solutions to counter the capability of the threat continues to be a challenge.

- IA is a highly dynamic area with no projected decrease in interest or the rate of change on the horizon. Accordingly, Navy continues to be quickly adaptive and responsive to meet today's and future challenges.

Those activities specific to the Marine Corps include the following:

- Marine Forces Computer Network Defense. The USMC Component of the JTF-CND established full operational capability in June 1999. USMC network defense provides global connectivity, intrusion detection, and protection with a

full capability to respond to and report computer-related events such as network intrusion attempts and probes.

- Implementation of PKI. Funding for FY00 USMC PKI was addressed in PBD-711, dated December 16, 1999. USMC-wide implementation of PKI will begin in the 2nd Qtr of FY00 with initial emphasis on establishing Local Registration Authorities (LRAs) and meeting the June 2000 deadline for issuance of server certificates. As of 31 December 1999, the Marine Corps has established the USMC Registration Authority within the Marine Corps Information Technology and Network Operations Center (MITNOC). The MITNOC is also currently acting as the Local Registration Authority for USMC personnel located in the National Capital Region. A draft USMC PKI Implementation Plan has been developed and is being staffed for comments/signature.

- Marine Corps Order (MCO) 5239.1 USMC IA order has been completed and staffed. Anticipate publication of this order during 2nd Quarter of FY00. This order will replace outdated Information Resources Management technical publications and will provide current USMC guidelines on IA.

- Completing Deputy Secretary of Defense-required IA certification and training of all SIPRNET system administrators and users. Also, anticipate required certification and training of all NIPRNET system administrators and users will be completed within Deputy Secretary of Defense-required timeline.

- MCO 5200.XX - USMC Certification and Accreditation (C&A) order has been completed and staffed. Anticipate publication of this order in 2nd Quarter of FY 00. This order delineates responsibilities for certifications and accreditation in the Marine Corps and provides those entities involved in this process the overarching guidance necessary to begin the C&A process.

- Established web security assessment policy. Established assessment teams, using Reserve forces in coordination with MITNOC, to conduct assessments of USMC websites to ensure compliance with DoD policy.

2.4.3. Department of the Air Force

The need to provide warfighters the information they need -- information they can trust – is a key component of the Air Force's Expeditionary Air Force concept. A strong IA program is the means to ensure an Air Expeditionary Force is able to apply air and space power in support of the Joint Force Air Component Commander's objectives. The Air Force has made several improvements in IA to ensure our continued success in assuring the availability, integrity, confidentiality, authenticity, and non-repudiation of Air Force information and information systems.

2.4.3.1. Mission Readiness.

- The Air Force made IA an integral part of its mission readiness criteria by implementing Status of Readiness and Training System reporting for its IA management and security infrastructure. This provides operational commanders

readiness posture visibility into our key DiD organizational elements. Further, Air Force published a change to AF Manual 10-206, Operational Reporting, requiring operational commanders to report significant IA-related events (network degradation, Information Operation Condition changes, and unauthorized system intrusions) to the Air Force Operations Center.

- To implement Presidential Decision Directive 63, Critical Infrastructure Protection, Air Force published a new Air Force Policy Document (AFPD). AFPD 10-24, Air Force CIP directs establishment of an Air Force CIP program, identifies lead organizations for CIP issues, and defines organizational roles and responsibilities.

- The Air Force began exploring follow-on uses for system information gathered for Year 2000 Rollover preparation. This information includes operationally assigned criticality levels for mission functions and information systems in use throughout the Service. It's anticipated that this data will play a crucial role in 2000 by helping to define required IA levels for our operationally critical systems.

2.4.3.2. IA Awareness

- Recognizing the importance of IA training, Air Force continued to expand and improve its IA training capabilities. All Air Force personnel receive training on IA through our Security Awareness Training and Evaluation program. During the Air Force's IA Month, Feb 99, over 200,000 Air Force personnel, made up of all ranks and specialties, received IA training via a Computer-Based Training (CBT) program. This increased AF personnel awareness of their IA responsibilities and improved knowledge about the cyber-based threat. The month's activities included various training programs and an extensive publicity campaign supported by senior AF leaders.

- In June, Air Force published interim guidance for implementing Information Operations Conditions (INFOCONs). This guidance implements the Chairman of the Joint Chiefs of Staff INFOCON policy. It provides Air Force units service-specific rules for establishing service-level INFOCONs, reporting lower-echelon INFOCON changes, and recommended actions to take at the different INFOCON levels. INFOCON processes will be formalized in an Air Force Instruction in 2000.

- In late 1999, the Air Force fielded an Internet-Based Training (IBT) capability; providing the mandatory annual IA training for all personnel using Air Force information systems as well as those operating or maintaining network computers. The IBT also includes user training on INFOCONs. Status of IA training is monitored by using the IBT registration and analysis engine that provides training metrics on demand. Additionally, Air Force is providing network management and network security tools training through both government technical schools and contracted training facilities. Mobile training teams provide just-in-time refresher training for deploying troops.

- To ensure commander awareness of IA issues, Air Force Audit Agency completed several IA-related audits. Air Force also instituted an Air Force Inspector General (IG) Special Interest Item (SII) for IA. The Air Force IG inspected over 50 units using the SII to assess the implementation of IA policies across the Service.

- Quarterly, the Director, Communications and Information provided the Secretary of the Air Force a briefing on IA items affecting the Air Force. The briefings included information on IA programs, audit results, status on the closure of critical computer vulnerabilities, and various other IA topics. The briefings helped ensure visibility into IA issues at the most senior levels of the Air Force. Having the Secretary's support and involvement was a benefit for all aspects of the Service's IA program.

2.4.3.3.   Defense-in-Depth

- Air Force continued to build on the capabilities of its three-tiered Network Management and Security architecture.   At the global level, the Air Force Network Operations Center (AFNOC) and the Air Force Computer Emergency Response Team (AFCERT) responded to network based threats like the Melissa computer virus to minimize impact to AF network operations. Managing the Air Force domain, AFNOC improved authentication requirements for 106 Service Delivery Points across the Air Force.   They also enhanced capabilities and improved security of 350 routers worldwide through software upgrades. AFCERT increased the number of Automated Security Incident Measurement System (ASIMS) IDS by 20 percent. New versions of the ASIMS software planned for release in 2000 and an expanded implementation strategy will bring increased functionality to our IDS capabilities. To keep up with the evolving threat, ASIMS attack signatures will continue to be updated with the latest hacking techniques to ensure early warning of attempted penetrations into AF networks.

- Network Operations and Security Centers (NOSCs) at each of our Major Commands (MAJCOMs) played an ever-increasing role in our IA processes. Overseeing network operations in each of their respective Area of Operations (AORs), NOSCs helped ensure network availability, monitor network operations, and responded to system intrusions/viruses.   In support of operations in Kosovo, the United States Air Forces Europe (USAFE) NOSC provided network operations and security services for Air Force units in theater.   The USAFE NOSCs capabilities were an integral part for the success of Air Force warfighters; ensuring information was available when and where it was needed.

- At the unit level, base Network Control Centers (NCCs) acted as the focal point for many IA issues. Working with the Wing IA office, NCCs provided network operations and security functions on the network front lines.   NCCs were responsible for assuring literally all network transactions occurring on Air Force installations. At the same time, they postured our networks for new threats by responding to over 50 network/system vulnerability advisories distributed by AFCERT.

- For several years, firewalls have been installed in AF NCCs worldwide. To enhance it's DiD capabilities, the Air Force installed additional firewalls and upgraded existing firewalls to new software versions at 27 locations. This project includes additional firewall training for local network operations personnel as well as the fielding of improved network management tools and a standard trouble ticketing system. The project will continue in calendar year 2000 and is scheduled for completion by early 2001, eventually enhancing firewall operations at all Air Force installations.

- With the increase in the use of the Internet, Air Force implemented several changes to improve the IA posture of our public web servers. A major improvement was the consolidation of public web servers outside our base firewalls, eliminating multiple servers and streamlining management of server security issues. Additionally, we removed from our websites sensitive material (operational information, privacy act data, etc) and implemented procedures to ensure review of all publicly accessible web pages before they're released. We plan to continue our web improvements by finishing development of a CBT for personnel involved in website development and maintenance.

- To help improve the supportability and security of new systems, Air Force began development of the Air Force Command, Control, Communications, Computers, and Intelligence Support Plan (C4ISP) policy. C4ISP policies will ensure C4I support elements are in place before systems are fielded, systems are compatible with the communications infrastructure, and help in programming decisions for infrastructure upgrades. A key output of the C4ISP will be a "certificate of networthiness" that indicates the system's suitability for use on Air Force networks. C4ISP policies will be in place early 2000.

- In support of OSD PKI initiatives, Air Force developed contract requirements for Air Force PKI implementation. The contract is in place for use in 2000. Additionally, Air Force developed several PKI related policies and an Air Force Instruction on PKI.

2.4.3.4. Computer Network Defense

- Air Force IA organizations continued to play a key role in Computer Network Defense (CND). The Commander, Air Force Forces to the JTF-CND worked with MAJCOM NOSCs to further address the evolving role of the JTF-CND. Air Force developed procedures to accomplish JTF-CND tasking and report required information back to appropriate organizations. In 2000, Air Force plans to develop an AFFOR Concept of Operations (CONOPS) to further delineate roles, responsibilities, and procedures for Service CND activities.

While the Air Force's network defenses are improving, so is the threat; it is real and dangerous. The DAF will continue to shore up the defenses through a well-funded and rigorous DiD program that will deliver the information and mission assurance for the expeditionary operations.

2.4.4. Joint Staff

2.4.4.1. Defense-in-Depth

The DiD concept has been further developed over the past year by a DoD working group and has produced an information-rich brochure now ready for print. The DiD approach integrates the capabilities of people, operations, and technology to establish multi-layer, multi-dimension protection - like the defenses of a castle. DiD employs mechanisms on successive layers that use a variety of methods at multiple locations. To prevent the potential breakdown of barriers and invasion of the innermost areas of the system, we must construct our defenses in successive layers and position safeguards at key sites throughout these layers. Guidance level detail will be developed in an upcoming revision to Chairman of the CJCSI 6510.01.

2.4.4.2. Information Assurance Panel

Several existing IA working groups were combined under a single panel under the MCEB in 1999. The panel charter was re-written and expanded in order to bring as many of the diverse and often over-lapping DoD IA panels, working groups, etc., under one central structure reporting to the MCEB. To accomplish this, the panel is now co-chaired by both the JCS/J6K Division Chief and the Director of the Defense Information Assurance Program (DIAP) and meets monthly. The panel membership was expanded as well to include planner level (0-6 or equivalent civilians) representatives from chartered members of the MCEB as well as the Agencies that previously made up the IAG. The IAP has tackled a host of critical issues this year.

2.4.4.3. IA Instructions Merger with Network Operations

The Joint Doctrine publication (JP 6-0) and the instruction governing IA (6510.01) are both due for revision. Joint Pub 6-0 is being re-written to focus on the concept of Network Operations (NETOPS). NETOPS is essentially the means to run the Global Information Grid and has three pillars, Information Assurance, Network Management and Information Dissemination Management. Consequently, the re-write of CJCSI 6510.01 (Defensive Information Operations) is being crafted to dovetail into the NETOPS concept. The new 6510.01 (Information Assurance through DiD) will be supplemented by other documents specifying readiness reporting instructions and Computer Network Defense issues relating to computer network incident reporting.

2.4.4.4. IA Readiness Metrics

The Joint Staff has developed an instruction that will supplement the new CJCSI 6510-01 (Information Assurance through DiD). This supplement will normalize IA readiness metrics into the Joint Monthly Readiness Review (JMRR) process and be used to periodically measure the IA operational readiness of combat, combat-support and combat services. These measures were developed over the past year and provide a tool for assessing operational readiness. The metrics can also be integrated into component operational readiness reporting.

2.4.4.5. CND Policy

Joint Staff has been working with an OSD led effort to define and write DoD computer network defense policy, roles and missions. The Joint Staff will further define CND guidance in the coming year to implement joint computer network defense operations through promulgation of a joint instruction supplementing its new parent document (CJCSI 6510.01, Information Assurance through DiD).

2.4.4.6. IA for NATO

The Joint Staff has been working on the NATO IA strategy. The future NATO strategy includes five recommendations to improve NATO's IA posture. The first recommendation is to establish a NATO Computer Emergency Response Team, which is similar to the U.S. Joint Task Force for Computer Network Defense. Second is to establish a NATO Vulnerability Assessment and Assistance Team, similar to our Service organizations that perform those roles. Thirdly, to establish a NATO Information Assurance Red Team to probe and identify NATO system vulnerabilities and initiate corrections. The fourth recommendation is to amend NATO policy to support "risk management" vice the traditional and impractical "risk avoidance" approach. This risk management approach is key to integrating NATO operations as we interconnect NATO/U.S./Allied systems. The final recommendation is to train NATO network users and systems administrators in a similar fashion to U.S. plans.

2.4.4.7. Information Operations Condition

In May 1999, the Joint Staff published definitions and procedures for INFOCON for use throughout the Department. The INFOCON process provides a structured, coordinated approach to defend against and react to adversarial attacks on DoD computer and telecommunication networks and systems. They are made up of sets of criteria that trigger response actions. INFOCONs allow commanders to uniformly heighten or reduce their defensive IA posture, enabling them to defend against computer network attacks (CNA) and to mitigate damage sustained to the DoD information infrastructure, including computer and telecommunications networks and systems.

2.4.4.8. Rules of Engagement

The Joint Staff has developed draft Rules of Engagement (ROE) for Information Operations, including defensive IO, which are currently under legal review. They are incorporated into the Joint Staff's Standing ROE instruction which specifies actions operational commanders are authorized to conduct in the execution and defense of their military operations. These ROE are critical for spelling out the appropriate responses to CNA (e.g., who has the authority to make decisions regarding these responses, and what notifications are required once a decision or action has been taken).

2.4.5. Commanders in Chief

All Commanders in Chief (CINCs) have recognized the criticality of IA and have healthy, aggressive programs. One of those programs has resulted in the Automated Intrusion Detection Environment-Advanced Concept Technology Demonstration (AIDE-ACTD). The AIDE-ACTD is expediting the fielding of an integrated detection environment and reporting capability. It will correlate intrusion events at local agency, CINC, and Joint command levels to tighten the detection grid and increase the success of identifying information warfare (IW) threats. Another high interest program is the prototype site for the Theater Network Operations and Theater C4ISR Coordination Center (TCCC). The TCCC provides the systems and network situation awareness necessary to effectively manage reliable and secure voice, data, and video services within a theater. This concept provides tremendous improvements in CINC IA visibility. Finally, work was begun to conduct the first ever global Computer Network Defense (CND) Exercise named "Apollo CND" in April 2000. This exercise is a direct result of Unified Command Plan 99 that assigned CND and CNA to the U.S. Space Command (USSPACECOM).

2.4.5.1. U.S. Central Command

From the start of 1999, the USCENTCOM has had a challenging year in IA. As the year began, Operation Desert Fox, the latest clash with Saddam, was drawing to a close. The continuing combat posture in Southwest Asia, due to heightened tensions with Iraq, has caused USCENTCOM to manage a delicate balance of its DIO posture against this almost constant state of operational readiness. However, 1999 was very successful in the DIO arena with the implementation of several DIO/IA plans and policies, as well as tackling the burden of accreditation in USCENTCOM's vast AOR.

During the spring and summer, the DIO Branch ushered in the implementation of INFOCONs for the command, as well as the drafting of DIO/IA CONOPS, and a DIO User's Guide.

USCENTCOM also teamed with the DISA Field Security Office (FSO) to attack the huge task of network accreditation. In the past, systems were accredited individually, but through some coordination and innovative thinking, a more complete site accreditation was completed, which included USCENTCOM HQ systems and also those systems operated by its rear component elements elsewhere on MacDill AFB. The accreditation of both SIPRNET and NIPRNET systems includes more than 3000 computer systems.

USCENTCOM DIO Branch personnel then deployed to Southwest Asia to assist in the accreditation of computer systems at Component Command Theater HQ and each of the additional Component AOR sites. They were joined by a team of seven DISA personnel that provided additional expertise to identify and fix network vulnerabilities. This effort was tied to the DoD Information Technology Security Certification and Accreditation Process' (DITSCAP's) Security Readiness Review (SRR) of systems, which is directly linked to each site's accreditation packages. This initial visit provided the baseline for future trips to achieve accreditation and ensure the latest IA techniques are used throughout the AOR.

During October 1999, USCENTCOM conducted a multi-national exercise in Egypt called "Bright Star". This is currently the world's largest coalition exercise and involved more than

38,000 U.S. and coalition soldiers, sailors, airmen, and marines. An IDS utilizing NetRanger and Border Guard was set-up on all Tier 1 network links. The system was then monitored for suspicious activity by the 9th Information Warfare Flight (IWF) from Shaw AFB. The 9th IWF was able to detect probes from unauthorized sources and block these sites from performing any malicious acts. Security on the deployed network was further tested on-site by personnel from the Systems and Network Attack Center of the NSA and the DISA FSO. DIO and IA will be incorporated into upcoming HQ exercises, such as "Internal Look" in November 2000.

The future of IA at USCENTCOM will continue to be fast-paced. From the day-to-day operations in Southwest Asia to the participation in joint and combined exercises, USCENTCOM will continue to strive for information superiority. Additional resources, particularly personnel and funding, are needed for our programs to mature. There is also a need for network defenders (i.e., JTF-CND) to work more closely with network management to ensure protection does not adversely impact operations. And finally, an improved threat assessment capability that can better forecast possible attacks against our networks and systems is needed.

2.4.5.2.   U.S. European Command

In 1999, the U.S. European Command (USEUCOM) had numerous activities critical to its ability to successfully execute operations and programs designed not only to respond to, but also to positively shape, the security environment.

- During Operation Noble Anvil, USEUCOM broke new ground in IA. Through changes to INFOCON levels, new practices to improve enclave boundary security, support from the Joint Communications Security (COMSEC) Monitoring Activity, and four significant IA teams provided real-world, operational IA support to USEUCOM's combat operations. Three of these teams came from NSA, and one was a joint NSA/DISA team. These efforts all served to enhance USEUCOM's IA posture by pointing out vulnerabilities and applying the appropriate countermeasures. The Lessons Learned from Operation Noble ANVIL are being shared across DoD to assist other commands in approaching similar problems.

- As part of the NSA/EUCOM Fellowship Program, two Training Needs Assessors determined USEUCOM needs in IA, relative to the duties of System Administrators, Information System Security Officers, Information System Security Managers, and general computer users. Assessments included HQ EUCOM, USAFE, USAREUR, and USNAVEUR, with over 80 individual interviews and four focus groups. The study reviewed extant courses. The result was a report detailing 18 general findings, 24 recommendations, and a detailed mapping of IA skills to specific tasks and careers ranging from military billet structures to specific training recommendations. The report also included listings of IA classes available worldwide.

- The EUCOM IA Master Plan serves as a living, evolving document to leverage and synchronize the best DoD/Joint, Service, MAJCOM and Component IA initiatives. The plan assesses our current environment, identifies a target

architecture and implementation strategy, and sets forth a framework to address 13 action plans for resolution of major theater IA issues through FY 2004.

- Based on lessons learned, an IA plan for Combined Endeavor 2000 was initiated early in the planning cycle. The plan addresses training and technical presentations, information systems and LAN/wide area network (WAN) testbed tests and demonstrations, as well as voluntary national use of IA implementation guidelines and self-evaluations.

- HQ USEUCOM hosted the first theater IA Conference to identify and develop action plans for the most pressing IA issues affecting the EUCOM theater. Demographics of the conference showed attendees included designated approval authorities, intelligence professionals, systems administrators, information system security managers and information system security officers, as well as IA specialties throughout several MAJCOMs and DISA. Key to this conference was the theater action team composed of key decision-makers for IA issues in the EUCOM theater. They reviewed action items collected in three track sessions, selected 20 as key to the EUCOM "roadmap" to the future of IA in theater, ranked each as high, medium and low priority, and then ascribed a primary action addressee to spearhead its resolution in the year 2000.

2.4.5.3. U.S. Joint Forces Command

Innovation and growth to keep pace with the increasing computer threat characterized information assurance (IA) at the USJFCOM in 1999. The challenges faced required innovation solutions and brought early and progressive changes in organization, resources, training, strategic planning and experimentation. The highlights in IA are provided below.

- The USJFCOM CND Watch Team was established to assist the DISA Regional Computer Emergency Response Team (CERT) at Scott AFB in protecting and providing a rapid response capability for the command's classified and unclassified networks. The CND Watch Team operationalized IA by publishing policy, guidance, and procedures, such as the Command's INFOCON instruction, the IA Appendix for the Command's OpOrder 2000, many Standard Operating Procedures for CND, virus protection and handling, and computer security broadcasts. The Good Password Formulation Policy and Guidance has significantly strengthened the security posture of unclassified and classified networks. The team supervised the following installations and upgrades: Joint Intrusion Detection System (JIDS) for Joint Forces Intelligence Command; Intrusion Misuse Deterrence System (IMDS) for the unclassified network; and a Gauntlet Smartwall firewall hardware and software upgrade for Y2K compliance. The Command was funded for more IA tools through the 1999 C2IP, which will enable this outstanding CND Watch Team to lead the establishment of a USJFCOM CERT in 2000.

- The USJFCOM IAVA website was designed, tested and launched. This on-line, collaborative, timesaving tool gathers and tracks IAVA responses from the 24 various IAVA points of contact throughout USJFCOM's Directorates, Sub-unified Commands and Joint Activities.

- USJFCOM was successful in training and certifying over 3,000 users and over 100 system administrators on both the classified and unclassified networks. IA training incorporated the information contained in the DISA INFOSEC CBT CD with an instructor-led class. All new users and system administrators are trained, tested and required to sign a letter acknowledging their appropriate roles and responsibilities for protecting the security of their systems. System administrators are required to complete Operational Information System Security CBT Volumes I and II, in addition to the DOD INFOSEC CBT.

- USJFCOM provided in depth security reviews of developing Advanced Concept Technology Demonstrations (ACTDs) in order to build security into the hardware and software while still in the development stages instead of after the fact. The ACTD actually shut down a system that was in violation of USJFCOM's security policy and forced the program management office to remedy the problems and publish appropriate guidance prior to becoming operational at USJFCOM.

2.4.5.4. U.S. Pacific Command

The U.S. Pacific Command (USPACOM) has recognized the criticality of IA and is continuing to develop healthy, aggressive programs. IA is included in the USPACOM prototype TCCC. The TCCC provides the systems and network situation awareness necessary to effectively manage reliable and secure voice, data, and video services within a theater. This concept provides tremendous improvements in CINC IA visibility. Work has begun on developing a Network Operations Center (NOC) to provide a robust platform for future network monitoring and IA.

IA awareness has improved tremendously throughout the theater and progress continues. New requirements continue to evolve as new systems continue to develop, integrate, and technology and policy evolve. Ongoing activities in the AOR include:

- Established permanent IA position in the TCCC.

- Established IA Common Operations Picture and battle rhythm.

- Developed IA policies and procedures for TCCC IA operations.

- Established IA web page containing IA messages, IAVAs, IA links, and timely bulletins.

- IA proved its mettle during the Melissa virus attack and has continued on a daily basis since the establishment of the TCCC in mid March 1999.

- Provided in depth analysis of CERT computer incident reports.

- Conducted daily IA briefing, providing visibility on theater activities.

- Developed theater guidance on IA education, training, and awareness products.

- Coordinated DITSCAP plans.

- Continued IA support to current operations and exercises.

- Continued on-going working relationship with Information Operations cell.

- Facilitated IA training, vulnerability assessment, and certification computer based training program in conjunction with DoD initiatives.

- Developed IA INFOCON theater impact assessments.

- Continued developing partnership with DARPA and NSA on CND/CNA activities.

- Hosted the USPACOM IA Conference held in Honolulu, Hawaii, May 1999, which160 personnel attended.

- Developed capability to analyze and correlate computer incidents across the AOR.

- Developed capability to monitor NIPRNET and SIPRNET strategic sensors as part of the Network Operations Initiative.

- Developed vulnerability assessment guidelines for analyzing sites undergoing probing and compromises.

- Acquired technologies to enhance vulnerability and penetration assessment as part of the TCCC Network Operations initiative.

- Improved education and awareness of IA.

Additionally, USCINCPAC took every opportunity to exercise and hone it's IA skill set. - USCINCPAC designed and implemented an IO exercise roadmap to institute a crawl-walk-run approach to IO within the Headquarters. The four exercises (Pacific Spectrum, Saratoga Thunder, Iron Hare, and Brazen Tsunami) were all designed and sequentially executed to leverage lessons learned from the previous exercise.

- **Pacific Spectrum**: A USCINCPAC-hosted, one-day tabletop seminar/exercise at the component three/four star/senior staff level (with FBI, NSA, CIA, DIA, and the Department of State included) aimed at probing USCINCPAC strategic decision making and contingency planning while under an IO attack. Pacific Spectrum laid the groundwork for the follow-on action officer level workshop, Saratoga Thunder.

- **Saratoga Thunder:** USCINCPAC hosted this workshop to validate command IO policies, procedures, and processes developed since Eligible Receiver '97. Participants included the HQ's IO Cell, JICPAC, Service Components, Sub-Unified Commands, JTF IO staffs, DIA, NSA, other Unified Commands, and Service CERTs. The goal was to validate, test, and refine USPACOM IO activities in a MSEL-driven scenario.

- **Iron Hare:** Iron Hare was a HQ USCINCPAC/JC2WC sponsored proof of concept IO exercise conducted at the Information Operations Technology Center (IOTC).

- **Brazen Tsunami**: A JICPAC designed and sponsored exercise to hone the intelligence support methodology for IO. The overarching goal was to exercise JICPAC's analytical response in a pre-hostility, IO-intensive environment and to raise JICPAC awareness of full-spectrum IO-related events.

USCINCPAC coordinated extensive IO play, complete CND, IA, and Defensive IO (DIO) ramifications, for Tier One exercises Reception Staging Onward Implementation '99, Ulchi Focus Lens '99, and Tempo Brave '00. The INFOCON policy, as well as the response measures, was used to drive decisions regarding IA and network security in the face of a simulated threat.

USCINCPAC is already gearing up for the Annual IA Conference for the Year 2000 and fully expects to have as active and challenging a year as 1999 was.

2.4.5.5.   U.S. Southern Command

The security of the U.S. Southern Command's (USSOUTHCOM's) mission depends on the survivability, integrity and authenticity of its information and information systems. USSOUTHCOM's IA Program uses a collaborative approach to form policy, processes, and practices which comply with DoD security regulations and to protect the information environment, detect attack, restore capabilities, and respond to attack. The Command's IA Program is augmented by specific technical systems protection aspects such as penetration testing, vulnerability assessments, computer defense against penetration, computer network mapping, red teaming and exercising. The Command's IA posture is consistently reviewed and addressed through the Integrated Priority List (IPL), Intelligence, Surveillance, Reconnaissance, CISA, the JMRR and the Joint Warfighting Command Assessment processes.

The following are examples of IA initiatives the Command pursued during the past year:

- The J6 IA Division is integrating IT reporting and monitoring functions with the J63 operations function in a combined effort to develop a Theater Network Coordination Center (TNCC). The primary mission of the TNCC is to provide the CINC J2, J3, and J6 with timely situational awareness of the operational and security status of the USSOUTHCOM information infrastructure by performing the following three core functions: network monitoring, systems monitoring, and security monitoring. The positioning of the TNCC will allow for a central point of contact for all C4I systems within the AOR and facilitate the expeditious completion of mission requirements.

- The J6 IA Division developed an IA Computer and Network Laboratory to facilitate testing and evaluation of information security products and practices, as well as network and security configuration. Without hands-on experience, it is difficult to accurately predict product performance or the ramifications of security advice promulgated by the command. The laboratory is essential to the Command's ability to appropriately gauge security risks, and countermeasures to these risks and is being made available to the entire IA community in USSOUTHCOM.

- Developed a comprehensive training program that satisfies ISSO and System Administrator (SA) certification requirements and that enhances the overall IA posture within USSOUTHCOM. Training is accomplished through commercially produced computer based training products from Learning Tree, as well as contracting local vendors for training. The Command-wide statistics, including the system administrators at remote locations throughout the AOR, for Level 1 Certification are: 130 NT System Administrators identified, of which 40 are certified; 13 NT Information System Security Manager (ISSM)/Information System Security Officers (ISSO) identified, of which four are certified; 92 UNIX System Administrators identified, of which 29 are certified; nine UNIX ISSM/ISSOs identified, of which five are certified. Sponsored six UNIX Security courses through a local commercial vendor, with a total of 91 students trained.

- Created a USSOUTHCOM specific INFOSEC CBT for system users. The interactive CBT incorporates a testing feature and automatic reporting to the J6 Network Security Branch for monitoring compliance with DoD policy. System users are required to pass the CBT within 30 days of their account activation and annually thereafter. User accounts are disabled for failure to complete the CBT as prescribed.

- Reinforced user awareness training through the monthly publication of "The Informer" newsletter. The newsletter focuses on relevant security issues to the Command. In addition, the headquarters has an annual Computer Security Day in April. Computer security posters and promotional items emphasize the importance of using good INFOSEC practices. This year's event included an Information Technology exposition with 15 vendors.

- Initiated the U.S. Military C4I enhancement plan, which entails the C&A activities for Security Assistance Organizations within the AOR. This effort concentrates on bringing NIPRNET connectivity to 32 separate military assistance organizations within the AOR and includes the installation of state-of-the-art computer systems, security configuration and testing, as well as the C&A effort. Further, the Command's IA functions provided significant IA support for USSOUTHCOM components relocating from Panama to Puerto Rico. Command assistance visits were conducted to assist with installation of firewalls and intrusion detection systems, and preparation of C&A packages.

- Supported full-spectrum IA to USSOUTHCOM exercises, including Fuertes Defensas 99 and Blue Advance 99. Most significantly is IA's participation in exercise Steel Puma, a full-spectrum IO effort supported by the Joint Staff, IOTC, DIA and JIOC. Part of the exercise will analyze non-U.S. Joint Intrusion Detection System data for vulnerability analysis, trends analysis and adversary detection. Additional personnel have allowed USSOUTHCOM to enhance its IA training, monitoring and exercise support.

- In an effort to enhance regional cooperation and information exchange among the countries in the USSOUTHCOM AOR, the IA communities in the Command have unified to promote commercial PKI standards. Utilizing PKI to address current regional security issues, the Command is participating in

protected intranets with host nations. Specifically tailored systems are being fielded to support these theater engagement initiatives.

- In an effort to better provide the Command with timely Indications and Warnings to support operations, the J2 IA community collaborated with the Command's IO Cell. Baseline adversary CNA capability assessment and I&W methodology and reporting vehicles were developed. These tools were successfully used to enhance the network defensive posture for the Command during several exercises and during humanitarian relief operations.

- The J2 IA community has taken an active role in the protection of the Command's information resources through tailored, timely intelligence products to support Command-wide INFOCON changes. These products have further enhanced defensive assessments for day-to-day network operations.

- The development and implementation of a JDISS NT Migration Plan presented many challenges for the J2 and J6 IA programs. Several partnering efforts resulted in singular efforts and commonality of security policies within the two communities. Most significantly is the agreement to produce a single IA Regulation for the command, which will combine the security requirements and policies for collateral and SI network operations.

2.4.5.6. U.S. Space Command

As the newly appointed DoD lead for Computer Network Defense (CND), the U.S. Space Command (USSPACECOM) has had a busy and productive year in 1999. In response to the President's 1999 Unified Command Plan that assigned CND to USSPACE Command on 1 October 1999 and CNA on October 1, 2000, USSPACECOM created an Activation Task Force to develop a DoD CND Implementation Plan (IPLAN). The plan was delivered to the Joint Staff on May 15, 1999 and approved by the Secretary of Defense in October 1999. A small-scale task force remains to develop the DoD CNA IPLAN and will be completed for official staffing by May 15, 2000. Additionally, CINCSPACE created a CND Concept of Operations to guide and focus DoD CND Unified commands, Services and Agencies in a unified DoD CND effort. This evolving document will be updated semi-annually to take advantage of lessons learned and identified effective CND information processes.

- While assuming the DoD CND mission, CINCSPACE assumed command of the newly created JTF-CND and will capitalize on their close relationship with the service CERTs to facilitate CND within DoD. They also assumed control of the newly named JIOC, formally the Joint Command and Control Warfare Center, in San Antonio, Texas. This organization will remain a full service joint Information Operations Organization supporting the needs of all CINCs.

- Continue to work closely with the Office of Secretary of Defense, the Joint Staff, and the Services to properly resource the new mission. While USSPACECOM has dedicated a few organic assets, they are in the process of filling the over 50 military and GS positions validated by the Joint Staff in a manpower validation board in September 1999. The additional 72 positions requested are being

51

reviewed as USSPACECOM fully engages in the CND mission and assumes the CNA mission in October 2000.

- As this critical DoD CND mission has evolved from a JTF-CND to a Unified Command, USSPACECOM has realized that the partnerships developed will be critical to leading into the future. They have been working closely with DISA, DIA, and NSA along with the all the Joint Staff elements. The DIAP will be a pivotal platform to reach key DoD CND players and USSPACECOM looks forward to a long-term relationship with them. Additionally, USSPACECOM has identified several business partners that not only share a common concern in this arena, but also will be instrumental in helping develop and implement a DiD strategy. The National Infrastructure Protection Center (NIPC), led by the FBI, is the key link into this community and USSPACECOM enjoys close ties developed through the JTF-CND.

- USSPACECOM looks forward to the DoD CND Challenge and executing a coordinated joint, combined, civil, and commercial effort to protect and defend critical information systems. USSPACECOM will lead DoD into the 21st century to maintain information superiority and give the warfighting forces the information dominance they need to fight and win.

2.4.5.7. U.S. Special Operations Command

One of the U.S. Special Operations Command's (USSOCOM's) missions is to organize and maintain an aggressive, effective IA Program that protects USSOCOM data and information assets enterprise-wide.

2.4.5.7.1. Division Overview

In 1998, the IA Division was established with a memorandum signed by RADM Steffens on 22 June 1998. The initial mission of the IA Division was to maintain current duties while adding the additional responsibility of securing the HQ USSOCOM networks. The CINC chose to expand this mission scope to secure all USSOCOM networks. With this new tasking, the IA Division was then responsible for organizing and determining the requirements to achieve this goal. Additional civilian, military, and contractor billets were added to the division. With the completion of the IA Master Plan in December 1998, the IA Division now had a plan of implementation to provide true network "DiD".

January 1999 began with the first USSOCOM IA Meeting, hosted by HQ USSOCOM with participation from the Joint Special Operations Command (JSOC) and the service components. The purpose of these meetings was to further information sharing and training. The initial session included training provided by the IA Technology Analysis Center in the area of Penetration Testing. Additional training was conducted for UNIX and Network Security, Computer Forensics, and instructions on performance as a Contracting Requirements Action Officer. To help the HQ USSOCOM Staff better understand and support JSOC and the service components, a staff assistance visit was conducted in February 1999. This visit helped set the stage for providing additional resources to JSOC and the Service Components in the areas of IA tools and contractor support.

2.4.5.7.2. IA Organizational Structure

The IA Division is divided into three functional areas of responsibility: technical security; COMSEC; and Plans and Policy. Military, government civilian, and contractor personnel combine to provide the necessary skills and support. Outside HQ USSOCOM, the addition of IA tasking increased the security workload of the components. To address this shortfall, the existing IA SETA contracting vehicle was used to provide an additional two contractors to the JSOC and each of the Service Components to augment the full-time government civilian and military personnel. The majority of the IA support at the JSOC and the Service Components is within the traditional communications support area (J6), although several organizations are exploring the combination of both intelligence (J2) and communications support (J6) functions in both information systems and security.

USSOCOM's mission of its technical security effort is ensuring the security of USSOCOM enterprise networks and hosts by establishing security configuration standards and assisting in the implementation and enforcement of compliance with those standards. In addition, the technical security effort tracks DoD and industry security advisories for vulnerability and countermeasure actions applicable to USSOCOM enterprise networks and hosts. Vulnerability assessment tests are conducted within the command's enterprise networks to identify vulnerabilities and investigate countermeasures capable of mitigating the risks.

Technical security is responsible for the performance of several functions: 1) Security Test and Evaluation for systems as part of the DITSCAP process; 2) mandated auditing requirements; 3) planning of new systems to ensure that security is integrated from the beginning; 4) technical reviews of new systems; 5) installation, maintenance, and monitoring of the Command's IA capabilities; 6) serving as the proponent of new IA capabilities for the Command; 7) participation in "change management" forums such as the Information Technology Requirements Review Board; 8) performance of technical security investigations; and 9) research of new technical security capabilities. Several new capabilities were fielded through the technical security effort. These included the DISA-furnished IMDS and Cisco's NetRanger/NetSonar on the unclassified networks. USSOCOM also integrated the Information Assurance Vulnerability Process on all its networks.

2.4.5.7.3. COMSEC Effort

USSOCOM's COMSEC Branch continues to forge ahead in the area of communications security. Summer 1999 saw the fielding of an Electronic Key Management System (EKMS) for distributing key materials throughout USSOCOM. The branch gained approval for continuing research in the area of CI-13, a cryptographic remote rekey initiative that will complement the existing EKMS program. On a daily basis, the COMSEC branch issues, maintains, and repairs controlled cryptographic equipment and secure facsimiles. The COMSEC Branch played a vital role in defining how USSOCOM will implement PKI within HQ USSOCOM, JSOC, and the service components through attendance at national level forums. The programming and maintaining of Fortezza cards for the Defense Messaging System (DMS) will increase as USSOCOM migrates to DMS. Finally, the COMSEC Branch continues to provide TEMPEST technical assistance.

2.4.5.7.4. Plans and Policy

The mission is to develop and maintain USSOCOM IA Program polices; ensure the adoption of the DoD standard accreditation process both within the headquarters and the components; maintain liaison with the Joint Staff for policy coordination; and monitor the development of national trends for computer security.

The Plans and Policy Branch develops and tracks computer security policies for HQ USSOCOM, JSOC and the Components. The first consolidated policies were signed in August 1999. Distribution to HQ USSOCOM, JSOC, and the components was achieved both through computer security training as directed by the Joint Staff and through distribution of the actual policies. Plans and policy retains the primary responsibility for implementing the accreditation process across all USSOCOM systems. It serves as the primary coordination point for IA review of systems proposed for fielding. They have the lead for implementing the IAVA process for USSOCOM. The Plans and Policy Branch also serves as the focal point for coordination between HQ, JSOC, the components, and the theater Special Operations Commands. Finally, they research the latest computer network defense/information assurance/defensive information operations developments, policies, and technologies. This capability was highlighted by the participation of USSOCOM in the Software Agents for OPSEC ACTD held this year.

2.4.5.8. U.S. Strategic Command

The U.S. Strategic Command (USSTRATCOM) continues to aggressively pursue programs to enhance IA across the command. The strategy is to be proactive and act with long-term impacts in mind. The initiatives below reflect this long-term focus.

- In May 1999, USSTRATCOM hosted the Omaha Cyber Security Conference. This event targeted CIOs and security managers in critical infrastructure companies in the Omaha, Nebraska, area. Over 100 representatives from Fortune 500 companies, state and municipal government; and others gathered at Offutt AFB to share in this first-of-a-kind conference. Two major corporations volunteered to continue the efforts to increase awareness in Omaha. A monthly meeting, the Cyber Security Forum, was established to share information between interested individuals and companies. Over 30 participants regularly attend these meetings where information security topics are discussed.

- As a direct result of local FBI agents' presentations at the Omaha Cyber Security Conference and at the Cyber Security Forums, an Omaha InfraGard Chapter was formed with several corporations coming on-board and more to follow. InfraGard will have two components--an Alert Network to allow members to communicate via secure email, and a website where computer security information and links to other security sites will be posted. Establishing the Omaha INFRAGUARD Chapter brings the NIPC a step closer to their goal of having a nationwide organization of public/private corporations sharing intrusions, known vulnerabilities, and corrective actions in order to protect our national information infrastructure.

- A collaborative partnership between USSTRATCOM and the Peter Kiewit Institute of Information Science, Technology and Engineering was formed to meet the ever-increasing need for information technology professionals in the Omaha area and around the nation. Realizing the importance of first-hand cyber security experience, over 20 of USSTRATCOM's information technology professionals volunteered their time to personally mentor Peter Kiewit Institute students. USSTRATCOM will hire six students as interns starting in January 2000, using the Office of Personnel Management's Student Temporary Employment Program (STEP).

- USSTRATCOM requested NSA and DISA to expand their Command Information Assurance Operations (IAO) reviews to include the Command's Task Forces (TFs). The expertise of both NSA and DISA staffs were vital to conducting an in-depth review of the Command's and its Task Forces' technical and administrative computer security architectures, protective mechanisms and methodologies. The result of this increased focus from NSA and DISA, along with that of USSTRATCOM personnel, allows USSTRATCOM to thoroughly address and assess the IA programs at each of its TFs. In turn, the TFs gained valuable training and insight into their security posture.

- Acting as the Operations Manager for the AIDE-ACTD, USSTRATCOM is working with DISA and the Air Force Research Laboratory to provide the DoD with a warning capability based upon "fusing" computer network attack information from multiple sources to create a "global" integrated intrusion detection system.   Knowledge gained from technical research and annual operational demonstrations is being leveraged into on-going DoD IA initiatives such as the IA Common Operations Procedures and the JTF-CND. AIDE will empower the participants to be aware of global CNA threats, to access locally-relevant information from a single platform, and to quickly choose a course-of-action appropriate to the level of attack.

- USSTRATCOM took the initiative to increase and enhance the protection of its information systems by implementing a software security tool called MimeSweeper. This security tool has greatly increased the Command's ability to respond to email threats, chain letters, and spam without temporarily denying its personnel the use of a critical communications resource.

- The USSTRATCOM CERT (STRATCERT) personnel took quick action to contain the Melissa virus. Their systematic response contained the outbreak and minimized system downtime. The steps taken subsequent to this virus attack resulted in the Command's ability to restore services ten hours before the JTF-CND directed that services could be brought back on-line.   Procedures developed at USSTRATCOM were passed on to Offutt AFB and Air Combat Command (ACC), enabling them to become the first ACC Air Force Base and Air Force Major Command to fully recover from the Melissa virus.

2.4.5.9. U.S. Transportation Command

In 1999, the U.S. Transportation Command (USTRANSCOM) continued to manage and operate a world class information systems security program. This included development of new security policies and procedures, development of a new, comprehensive security education, training, and awareness program, and providing security engineering guidance to internal and external organizations. Other day-to-day missions included providing technical security guidance and evaluating emerging programs for compliance, and providing secure information systems support to USTRANSCOM and other Defense Transportation System missions.

Of particular note was the significant progress made in the implementation of our overarching DiD security strategy known as Information Assurance/Information Protect (IA/IP). The IA/IP incorporates both technical and non-technical solutions in an effort to extend the airtight network security enjoyed by the headquarters to the USTRANSCOM Component Commands. Highlights of the IA/IP implementation include:

- Placement of security engineers at two of the three USTC Components, AMC and MTMC

- Secured $500K funding and completed design of new Network Management Center

- Purchase of approximately $200,000 worth of IA hardware and software to enhance capabilities

Other major USTRANSCOM achievements included:

- Enhanced depth and credibility of the Information Systems Security Branch by increasing IA staff by six people, including the addition of liaison representatives from NSA and DISA.

- Conducted USTRANSCOM's first-ever dedicated INFOSEC exercises. The highly successful exercises known as Paradise Express I and II involved the entire Scott AFB community (PE I), and the component commands (PE II). The exercises significantly enhanced the training of security personnel and served to validate existing tactics, techniques, and procedures. PE I and PE II were the first two phases in an overall "crawl-walk-run" philosophy which will culminate in a multi-command exercise which will combine PE III with USTRANSCOM's Turbo Challenge 2000, and USSPACECOM's Apollo CND.

- Initiated actions to separate the USTC domain from the rest of the base networks to reduce vulnerability of USTRANSCOM networks.

- Participated in DISA's PKI pilot program.

- Continued to deploy and upgrade IA tools to protect the Defense Travel System from cyber attack.

2.4.6. National Security Agency

The National Security Agency (NSA) 1999 IA activities were focused on implementation of the layered assurance strategy construct for DiD. These activities were focused in the following principal areas:

- Continued evolution of an IATF that advocate the concept for DoD's IA architecture and technology, identifies the gaps that currently exist, serves as the foundation for creation of supporting technical specifications for each of the DiD layers. In addition, it provides the architectural framework for creation of protection profiles by which IA-relevant technology can be assessed and procured. As part of the IATF effort, NSA sponsors the IATF Forum, composed of both Government and industry participants. The IATF fosters dialog that may result in the availability of the commercial security-enabled technology required for creating security solutions to address emergent DoD user IA requirements. NSA published two iterative versions of the IATF document, hosted nine IATF Forums to advance the framework concept, developed and published supporting technical specifications for firewalls, remote access, operating systems, key management, and applications in support of three of the DiD layers.

- Generation of Protection Profiles (PP) that establish the criteria and standards by which IA relevant technology products can be assessed and procured. NSA performed security evaluations and established PPs for key technologies required to implement IA security, e.g., firewalls, routers, guards, PKI applications, etc.

- Establishment of processes, procedures, and standards required to certify commercial laboratories to support the evaluation of commercial security-enabled products based upon the Common Criteria (CC) for IT Security, an internationally accepted criteria for developing and evaluating the security of IT products and systems. NSA developed the scheme for the joint NSA/NIST National Information Assurance Partnership (NIAP) commercial laboratory evaluation program and continued further refinement of the Common Criteria. Concurrently, it directed the operations of the interim NSA sponsored laboratory evaluation program called the Trust Technology Assessment Program. (Currently there are seven approved commercial laboratories conducting ten on-going product evaluations.) The NIAP also conducted NSA product evaluations under the Trusted Product Evaluation Program, based on the Orange Book criteria which will be replaced by the Common Criteria.

- Continued Government development and evaluation of selected IA technologies to address COTS technology gaps and commercial security shortfalls to support higher IA requirements in accordance with the DiD strategy and IATF. NSA continued its development and evaluation initiatives in attack sensing, warning and response, wireless, key management, NC2, space, satellite, weapons, telephony, ATM, Synchronous Optical Networks, and IP in-line network encryption technology, etc.

- Implementation of IA engineering processes to generate and test a steady stream of reusable solutions that can be certified, deployed and accredited successfully.

NSA supported efforts to develop and evaluate reusable IA solutions in the areas of Electronic Commerce/Electronic Data Interchanges (EC/EDI), two-level web security, Virtual Private Networks (VPN), remote access, and secure email.

- Provision of system security engineering support to specific programs within the DoD and Intelligence Community in accordance with the DiD strategy and IATF architecture. Major programs supported include: USPACOM Multi-Domain Dissemination Server; NSA's Unified Cryptologic Architecture (UCA); the Joint Staff's SABI; DoD's DMS; NSA's internal network - NSA-NET; the IC's Intelligence Link; DoD's Global Command and Control System (GCCS); and Air Force's F-22 program. System security engineering support includes security guidance and consulting, development of IA policies and plans, systems security requirements identification and definition in Common Criteria language, Protection Profiles, security solution generation, test and evaluation, and security certification and accreditation support.

- Performance of security infrastructure operations (i.e., key management and PKI) for all DoD fielded IA products and systems. Provided approximately 2.5M individual key products, to include physical, electronic key and rekey, and PKI certificates.

- Continued focus in defensive information operations (DIO) and technical support within NSA in three very broad categories: (1) Force Protection, Monitoring and Analysis; (2) Operational Readiness Support; and (3) National Security Incident Response Center. NSA DIO provided force protection monitoring, OPSEC and vulnerability assessments, threat advisories, deep technical analysis, fielded network system and facility evaluations and similar support to military combat operations in Kosovo and South West Asia and to operational counter-drug activities of the U.S. Coast Guard, CIA, NRO, DIA, CINC's and other major commands. NSA DIO also provided extensive operational readiness support through Red Team activities during military command exercises and real-world events. Analytic results of cyber intrusions, incidents and events affecting national security systems and operations were reported daily to a broad audience and comparable technical support was provided to federal law enforcement agencies countering significant events.

- Establishment of, at the direction of the Deputy Secretary of Defense in April 1999, along with DISA the DoD PKI PMO to plan the Department's activities for PKI implementation within DoD. The PMO has drafted, coordinated, and finalized the three operating documents that will assist in PKI implementation: the PKI Roadmap; the PKI X.509 Certificate Policy (CP); and the PKI Implementation Plan. Pending availability of the targeted PKI described in these documents, the PMO initiated a security assessment of the Class 3 Release 2 PKI System by SA and approved three vendors to serve as Interim External Certificate Authorities (ECA) and to sell Class 3 certificates to external (non-DoD) entities that need to conduct electronic commerce and business with DoD. The PMO also initiated development of the Class 4 Target PKI architecture, scheduled for release in the first quarter of CY2000.

- Continued operation of the DoD's INFOSEC Research and Technology Program to ensure that research in leading edge technology drives the development of future IA solutions and advances the technological state-of-the-art. NSA focused research activities in cryptography, active network defense, secure communications, and secure network management. Examples of these activities include: development of new cryptography for emerging technologies; the completion of several research models of autonomous agents for network detection; development of a mapping and monitoring tool for ATM networks; development of a 1200 bits per second voice coder in support of U.S. and NATO programs; development of a wireless local LAN prototype; design and fabrication of high speed integrated circuits for use in ATM applications; and the development of security protocols for use in exchanging keys over the Internet.

2.4.7. Defense Information Systems Agency

Joint Vision 2010 requires information superiority, assumes a real-time, unrestricted flow of information, and cites the protection of the capability to conduct information operations as one of the most important challenges in the future. The Defense Information Systems Agency (DISA) is responsible for managing and operating the Defense Information Infrastructure (DII) and, as such, has the role to ensure the DII contains adequate protection against attack and that robust dynamic network capabilities are maintained to ensure continued availability to sustain warfighting efforts. The DISA IA program responsibility includes the DoD-wide security architecture, technical implementation strategy and current security operations – implemented proactively, routinely, and in response to crisis. DISA is implementing a DiD strategy that provides layered protection by leveraging architecture and technology to provide technical network and systems defense in support of warfighters, while managing teamwork, products, security and services to achieve national security objectives. DISA plans, acquires, integrates, implements, and supports full spectrum, interoperable IA products, services, and processes in support of the CINCs, Services, and Agencies. The following is a list of activities accomplished by DISA in 1999, categorized by the major functional areas of DISA's IA Strategic Plan:

2.4.7.1. Architecture and Technology.

The amount of audit data captured at the various information technology centers has significantly increased and will continue to do so. To accommodate this growth, DISA fielded a prototype audit server that is designed to efficiently store and manage audit data in a mid-tier environment and protect it from loss or damage.

The DISA sponsored DoD-wide anti-virus program provides two standard products to the Department under an enterprise license, as well as fielding various GOTS intrusion detection products. These product lines have improved the Department's ability to detect, deter, and respond to malicious code and activity on DoD networks, enclaves, and workstations.

Implementing end-to-end of application-to-application encryption often provides protection to the warfighters' applications and data. End-to-end encryption has been employed successfully by the military for decades. Application-to-application encryption is now commercially available and has come into relatively widespread use as users of personal computers seek to secure word processing documents and other data files without having to

encrypt all other applications. The strategy of using asymmetric or PK encryption has attained widespread popularity. Currently, the most reliable and trustworthy means of implementing this strategy is by creation of a PKI. DISA operates and maintains the DoD Medium Assurance Pilot PKI. Currently, more than 23,000 certificates have been issued. Enhancements have been made to improve the ease of use and enhance the certificate registration process.

DISA's Secure Web Access (SWA) system employs WorldWide Web technology to meet security requirements for DoD users transmitting sensitive, unclassified information over the NIPRNET. The SWA capability reduces this vulnerability by encrypting the message traffic between the client and the SWA server, including all userids and passwords, through a combination of PK and secret key cryptography. The SWA platform is located within the DoD Defense MegaCenter (DMC) where it connects to a mainframe computer that hosts the applications and databases for the user's transactions. Customers using Defense Finance and Accounting System (DFAS) Standard Accounting and Reporting System, Defense Civilian Pay System, the Navy's Financial and Air Clearance Transportation System, and the Navy Facility Support Office are securely accessing the mainframe computers via a web interface and secure web protocols. In FY99, the SWA system was successfully installed and implemented at the DMC, Mechanicsburg, Pennsylvania.

DISA continues to support local intrusion detection capabilities. Deployed the Automated Intrusion Detection Environment (AIDE) to nine CINC, Service, and Agency locations. This provides a security view of disparate sensor information on common platforms. Protection devices (e.g., firewalls) intrusion devices (e.g., Joint Intrusion Detection Systems) and host-based monitoring software, (e.g., Computer Misuse Detection System) provided data feeds to the AIDE. An IA exercise was conducted in September 1999 to demonstrate the ability to detect, correlate, visualize, and report IA events against the instrumented locations. The AIDE provided visualization, basic correlation, and forwarded the information to the regional and global NOSC.

DISA fielded an initial IA detect and respond capability federated with the Joint DII C2 System-Deployed to the Joint Communications and Support Element at MacDill AFB. This provides additional IA attributes of integrity, availability, confidentiality, and accountability for the Deployed JTF Commanders, CINCs, and JTF Component Commanders in deliberate/crisis action planning and when contingency/exercise execution is required.

DISA installed and implemented an Incident Operations Report Database for the JTF-CND. The JTF-CND requires a correlation and analysis system to deliver course-of-action options based on network security events and incident reporting. This requires developing a data storage/management/retrieval model for obtaining event and incident reports, and accessing information required to develop course-of-action options. This installation provides the first phase of this project.

Multiple Security Levels (MSL) includes secure interoperability between networks of differing classifications (i.e., NIPRNET, SIPRNET, coalition networks) in support of DoD operational and strategic missions via department C4I programs. DISA provides Command and Control Guards (C2G) and the N-Level Workstation. DISA implemented 14 C2G upgrades for C/S/As, including substantial Y2K system upgrades. In May 1999 DISA fielded an MSL solution allowing Global Command and Control System-Army (GCCS-A)-to-Coalition secure data exchange for warfighting missions in the Republic of Korea. For

the first time, Ground Order of Battle information was passed to a coalition information system. In June 1999, coalition interoperability requirements were satisfied through DISA's MSL development and support for CINC North American Aerospace Defense Command/SPACECOM allowing secure data exchange of Common Operational Picture data for U.S. and Canadian Forces. DISA also provided numerous Y2K upgrades for N-Level Workstations in USJFCOM, USEUCOM, USPACOM and USSOCOM.

The DII objective is to provide an uninterrupted flow of information to the warfighter at anytime, in any theater of operations, and under any conditions, either is peacetime of during periods of crisis. The principle concept encompassing DII information flow will be an interoperable, dynamic, and cohesive information environment capable of supporting multiple information ingress and egress systems and technologies. The plug-and-play operational concept of the DII presents some risks and the interconnection of networked DoD systems presents the concept of shared risk – risk accepted by one is subsequently imposed on all. These risks must be managed and the protective measures to be applied must be commensurate with the value of information being protected. In FY99 DISA improved the Defense Information Systems Network (DISN) in the following areas:

Asynchronous Transfer Mode (ATM) is emerging as the primary networking technology for next generation, multi-media communications. Network availability requires protection of the links both between components (router-to-router) and between network management centers and components (center-to-switch/router) DISA provided secure ATM switch management through fielding a cryptographic token-based identification and authentication mechanism to control access.

DISA teamed with industry and academia to secure the Domain Name Service (DNS) system. Vulnerabilities that relate to denial of service attacks, unauthorized access, and unauthorized alteration of DoD servers are being eliminated. DISA established a standardized Common Operating Environment (COE) configuration management of DNS servers for the DII and identification and authentication for DNS transactions. In June 1999, DISA released a secure version of the DNS software BIND version 8.1.2 segmented on the DII COE for DoD communities.

The DII COE provides the software foundation on which the majority of all DoD Command and Control Systems (GCCS, GCSS, etc.) are built. DISA refined security assessment tools and guidance for securing the GCCS hosts and applications through DII security services, including general security services, application program interfaces, and COE lock-down guidance. In addition, DISA security enhancements to the COE significantly improved the warfighter's capabilities to operate command and control systems in a hostile information warfare environment.

2.4.7.2. Warfighter Support

DISA is a key agency for providing IT and IA support to the CINCs. The CINCs rely on DISA to provide teams of functional experts for comprehensive assessments of their specific enclave vulnerabilities. During 1999, IA reviews were conducted for seven major CINC headquarters and one Unified Command headquarters. These system-by-system technical reviews, penetration tests, exercise support, IA training, and certification support

have increased the security readiness posture of the DoD CINC component headquarters will also receive IA reviews in 2000.

DISA provided direct support to the CONUS CINCs through IA Representatives. Their role is key to supporting IA coordination, planning, and operations during security readiness reviews, tool deployments, IA exercises, and contingency operations. Security resolution coordination support is also provided to assist with certification and accreditation. Their direct interface with the CINC staff, combined with their coordination with the Global Network Operations and Security Center (GNOSC) and Regional Computer Emergency Response Teams (RCERTs), facilitates DISA's ability to meet the warfighters requirements.

DISA conducted security certification and accreditation in accordance with DoD Instruction 5200.40, the "Defense Information Technology Certification and Accreditation Process (DITSCAP)." Security certification and accreditations were performed on the Defense Message System Release 2.1 and 2.2, the DII High Assurance Guard and other DMS Infrastructure components. Security certification and accreditation support was also provided GCCS, GCSS, the DISN Bandwidth Manager, video and transmission services, and other DoD information technologies.

DISA chairs the DISN Security Accreditation Working Group composed of DIA, NSA, DISA, JS, CIA, the Military Services and Defense Agencies.

SIPRNET Connection Approval Process (CAP) was used for 201 new connections, 10 on-site inspections, and over 200 remote (electronic) inspections. The SIPRNET CAP provides network integrity through standard security connection requirements and dynamic and static assessment of local and infrastructure security posture.

2.4.7.3. Technical Network and System Defense.

Postured a world-class DoD Computer Emergency Response Team (DoD CERT) providing a broad range of technical computer network defense support to CINC, Services and Agencies. Provided incident handling, malicious code analysis, and reporting assistance to the DoD community handling large-scale incidents such as Moonlight Maze and the Melissa outbreak.

Integrated CERT functions with the traditional network management functions which has produced a strong technical base to identify and resolve complex network issues including denial of service attacks, and network congestion/configuration issues. The DoD CERT structure supports strategic cyber threats. Organizational emphasis is placed on the strategic analysis of vulnerability and attack profiles, establishing a vulnerability management process, to include malicious code, as well as long range planning and CINC exercise support. Provided the JTF-CND with technical expertise to aid in the identification of strategic CND issues which could negatively impact on-going military operations around the globe.

The DoD CERT serves as the DoD coordination center for CND issues through a collaborative relationship with industry, law enforcement, and national intelligence organizations. DISA maintains a strong relationship with the CERT Coordination Center and the International Forum for Incident Response and Security Teams. During the past

year the DoD CERT has participated in the research, analysis, discussions, and development of numerous countermeasures to mitigate risk to the shared computing environment.

Established five RCERTs to support the CINCs and DoD agencies by providing incident handling and reporting assistance. These RCERTs are co-located with the DISA Regional Network Operations and Security Centers (RNOSC) to provide a common view of the health and stability of the DII. These teams analyze intrusion detection and incident reporting data to develop theater-wide IA reports. RCERTS operate within the RNOSCs in the Pacific, European, and Central Theaters with two locations in the continental United States. The co-location of the RCERTs with the RNOSC provided a common view of the health and stability of the DII.

Integrated network management and CND by establishing a CND Assessment Team (CND AT) that conducts the first level of triage for computer incidents and anti-virus software support. This team directly supports the DoD CERT and indirectly supports the JTF-CND during CND operations, exercises, and contingencies. Provided rudimentary, diverse sensor monitoring during the annual AIDE-ACTD. Identified operational requirements for a more robust, real-time intrusion detection monitoring and assessment capability. Developed and implemented a detailed training plan to certify CND AT members to meet DISA Level 1 Systems Administrator standard.

Implemented a sensor grid management process for the deployed JIDS based on the five systems management disciplines (i.e., fault, configuration, accounting, performance, and security management). Optimized the sensor gird performance by redistributing the internal program responsibilities between: the GNOSC/IA Operations for DII operations, fault monitoring, performance assessment, and requirements analysis; the DoD CERT for configuration management and requirements validation; and the FSO for accounting and security management. In addition, provided greater responsibility to the RCERTs for data analysis and sensor performance. Developed a capability to monitor over 80 SIPRNET and NIPRNET strategic sensors from the GNOSC. Upgraded all of the DoD sensors for Y2K compliance. Established protected website for sensor placement network diagrams and information on other intrusion detection technology. Identified critical C4 resources for monitoring malicious behavior and prioritized future deployments for network sensors to include a real-time component.

2.4.7.4. Information Assurance Center of Excellence.

DISA developed Security Technical Implementation Guides (STIGs) for every prevalent operating system within DoD. These guides are the foundation of DISA's review programs and have been made available to all of DoD through a secure website.

DISA provided IA education, training and awareness (ETA) products. This OASD(C3I) activity provided CINC, Service, and Agency personnel both classroom training and interactive multimedia computer-based training (CBT) and awareness to support certification of system administrators and users. Products developed and disseminated by the DISA IA Program Management Office (IPMO) are being used in Service schools and training organizations, by unit trainers to support IA training and awareness in the field, and by individuals seeking to enhance their IA knowledge and skills.

DISA ETA initiatives included production of Public Key Infrastructure CBT products; the CINDI Award-winning Cyberprotect CBT, and an innovative IA training exercise for system administrators, information system security officers and managers, and other IA personnel to support the DoD mandate for Certified System Administrators, updated UNIX Security and Windows NT Security for a System Administrators classroom course and began transition to CBT; under the IPMO Franchise Program, qualified U.S. Army Reserve trainers at Ft McCoy, Wisconsin to deliver DITSCAP and Introduction to Information System Security courses; disseminated 100,000 IA training and awareness CBTs and videos within DoD and Federal government-wide, up from 30,000 in FY98; in support of DoD and Federal outreach programs to industry and academia, obtained a DoD open dissemination release for most CBTs, and facilitated making the products available to the general public through the National Technical Information Service of the Department of Commerce; continued to facilitate integration of INFOSEC training and awareness classroom materials, videos and CDs into Service/Agency school house curriculums. These serve as pre-requisites to establish baseline level of knowledge prior to class, and are being used to reduced class-room time required to cover the same amount of information, OR allow additional hands-on training, AND/OR permit addition of new material without increasing course length.

DISA participated in the Information Assurance and Information Technology Human Resources, Insider Threat, and Website Security IPTs.

- DISA developed and updated DITSCAP Instruction and associated Application Guide, in coordination with OASD(C3I)/I&IA. The DITSCAP provides guidance for the SIPRNET CAP, NIPRNET CAP, and certification requirements for DoD programs and systems. The DITSCAP Implementation Guide, also known as the Application Document, is being formally coordinated with all Services and Agencies. Initial comments have been provided and the proposed changes are being harmonized with the DITSCAP. DISA was requested to adapt the DISCAP to a government-wide focus. A draft National Information Assurance Certification and Accreditation Process was developed and is in the staffing process.

2.4.8. Defense Logistics Agency

The Defense Logistics Agency (DLA) made significant progress in the area of IA during 1999. Specific accomplishments are as follows:

- Established a headquarters IA Team under the purview of the Chief Information Officer. The team is divided into four groups: Policy Integration and Human Resources, Readiness Assessment, Operational Environment, and Product Development and Standards.

- Established the DLA Computer Emergency Response Team (DLA CERT) in Columbus, Ohio, with links to the DoD and Services CERTs. Published the DLA CERT Handling Procedures and distributed it to all DLA field activities.

- Provided security awareness products to all DLA activities, and conducted several security awareness sessions for employees.

- Certified all System Administrators responsible for SIPRNET connections, in compliance with DoD mandate.

- Supported the DoD PKI. Participated in the writing of policy and implementation plan for PKI. Registration Authorities/Local Registration Authorities received training and began issuing DoD PKI certificates to employees. Participated in the PKI FEA.

- Completed the installation of firewalls at all primary level field activities and began covering the secondary locations.

- Began installing intrusion detection systems and contracted for enterprise licensing of intrusion detection software. It is DLA policy that each firewall location will have an intrusion detection system installed.

- Instituted anti-virus software at mail server level as well as to the personal computer level.

- Wrote DLA INFOCON policy.

- Conducted the first CIO IA Conference for Information System Security Officers and System Administrators. Next one is currently scheduled for the Spring 2000 timeframe.

- Participated in the GNIE, now the GIG, IA Policy working panel.

- Began the DITSCAP for the certification and accreditation of all systems, networks and web pages within DLA.

- Drafted CIO IA policy letters on firewalls, intrusion detection, virus handling, hotlists, performance reviews, Windows NT and configuration management.

- Implemented the DoD IAVA system within the field activities, monitored by the DLA CERT.

- Published the DLA IA Plan.

- Conducted vulnerability assessments of several DLA activities.

- Acquired Secure Sockets Layer (SSL) to replace telnet access and connection methods.

- Acquired Internet Security Scanner for ISSOs to use to scan systems for vulnerabilities.

- Began the establishment of an IA Program Review Team to perform "internal checks" on our IA posture at our field activities.

- Due to rapidly changing IA needs and awareness, DLA has undertaken a complete rewrite of corporate level IA Policy document. This DLA Policy Directive, now in coordination, will derive its guidance from Agency and

Department strategic guidance and it will serve as the umbrella document for a host of implementing guides, handbooks, and instructions. Anticipate finalization early in the calendar year 2000.

2.4.8.1. Assessment

Since the functional realignment of the IA function from Command Security to the CIO, DLA has made progress in the IA area; however there is still a long way to go. With the DLA CERT established, and the use of IA tools such as firewalls and intrusion detection devices, DLA has improved its ability to identify intrusions and attempted intrusions to its systems. However, monitoring these systems and reviewing logs is very cumbersome with the limited resources and tools available. DLA plans to continue to install firewalls and intrusion detection systems at secondary locations as resources permit, and to hire contractor support to assist in interpreting information provided by these systems.

DLA is convinced that education, training and awareness of all employees are a necessity. DLA is developing a training program within the command that will identify for employees those classes necessary in the information age.

The agency has participated in as many OSD-level IA teams as possible. DLA is a unique Agency, with much to offer through participation in these teams, and through its assistance with the development of guidance and policy for the DoD.

Certification and accreditation (and some re-accreditation) activities are scheduled for all DLA systems, networks and websites

DLA conducted the first IA Conference to bring the ISSOs and system administrators up-to-date on OSD's guidance and policy.

2.4.8.2. Issues: Funding, Priorities, and Policies

As with other agencies, resource availability has posed significant challenges to DLA in 1999 and will continue to do so in the future. New requirements must be evaluated in terms of priorities and risk management, as well as unique challenges faced by the organization. .Examples of these challenges include: data aggregation issues in the networked environment; administering to Foreign Nationals when issuing PKI certificates; and administering DLA systems overseas.

2.4.9. Ballistic Missile Defense Organization

The Ballistic Missile Defense Organization (BMDO) is the only Acquisition Agency with an IA Program directed at Executive Agents who build and test missile defense systems. It contributes to the DiD strategy by assessments of network security using a regional approach, called Collaborative Defense, which combines industrial security for contractors, Executing Agent network security programs, and BMDO programs. These three elements have improved network defense through the following:

- The funding and operation of the Secondary Heuristic Analysis for Defensive On-Line Warfare (SHADOW), a joint-Service intrusion detection system. The system is oriented to discovery of previously unknown attack techniques. SHADOW sensors are located at Service sites and provide a broadband analysis of intrusions to DISA. SHADOW won the Government Technology Leadership Award of the CIO Council in December 1998.

- A joint assessment of the Huntsville, Alabama, networks centered around Redstone Arsenal. This combined persons from industry, Army Material Command, BMDO, and Defense Security Service. This collaborative approach was well received and resulted in a considerable improvement in awareness and network defense posture. Most improved was the Air and Missile Command which now has a computer emergency response function, quadrupled the resources committed to IA, and much improved network visibility. This concept demonstrates that regional assessment and collaborative funding of defense measures from the network hubs to local desktops can make considerable improvement.

- The training of Systems Administrators was extended to Network Security Professionalization resulting in 70% of the network security workforce, both contractor and government, obtaining professional certifications as Certified Information Systems Security Professionals with the remainder being certified through local testing. Specialized incident handling training was given and the Security and Network Security professional organization adopted the product as a commercial training package.

- Incident handling, network security administration across multiple networks, and day-to-day exercise and test support services are coordinated through bi-monthly video teleconferences between seven sites that comprise the major network hubs. New network attack approaches are disseminated and explained, operational issues discussed face-to-face, and contractor issues are raised and resolved.

2.4.10. Defense Finance and Accounting Service

A PKI will become the critical underpinning of the DFASs IA capabilities and will be a vital element in achieving a secure IA posture for the DFAS Corporate Information Infrastructure. Accordingly, during FY 1999, DFAS further positioned itself to rely upon the DoD PKI for the future implementation of PK-enabled applications. DFAS equipped and trained a Local Registration Authority at each of the five DFAS Centers, at Headquarters, and at many of the operating locations, enabling end users of several PKI pilot applications to receive DoD-issued PK certificates. During the fiscal year, more than 1,500 certificates were requested and issued to DFAS users of the Electronic Document Access program. A provisional PKI lab also was established in the Infrastructure Services Organization allowing DFAS to evaluate several vendors' COTS products including application programming interfaces and various implementations of digital signature, registration, directory, and encryption services.

To improve the IA posture of the internal network infrastructure, DFAS network administrators replaced direct modem access by increasing the use of Terminal Access

Control devices, eliminating a major potential avenue of attack into the network. Although not yet completed, DFAS collaborated with DISA to test various implementation options for encrypting all data transmission between DFAS locations and all Defense Megacenters.

To provide an improved "detect and monitor" capability, DFAS procured and installed an automated, real-time intrusion detection capability. With this capability, an intrusion by a hacker or unauthorized person is more reliably detected and immediately reported to the DFAS network-monitoring center. Every mid-tier platform, router, and Novell and NT server, including the web servers, is covered for detecting and reporting an intrusion attempt.

To enhance DFAS education, training, and awareness efforts, an IA Training and Certification Plan for the agency was developed and approved, and currently is being executed so that every user, administrator, and maintainer of the DFAS network is formally certified by December 2000. In addition, DFAS technical and IA personnel have attended multiple security conferences, and an internal Information Security Manager Conference was conducted for the benefit of all ISMs in DFAS. The DFAS Vulnerability Assessment Team continued to regularly perform network scans, looking for and correcting weaknesses and vulnerabilities in the network infrastructure.

To better identify vulnerabilities and risks to DFAS applications through the certification and accreditation process, program managers of several major systems have either converted their current accreditation packages or began new efforts to certify and accredit their systems using the DITSCAP. This effort is an on-going initiative until all mission critical systems have received a final accreditation in full conformance with the DITSCAP.

2.4.11. Defense Intelligence Agency

The DIA has conducted the following actions:

- Increased the number of IA personnel by 200% (from 8 to 24) and improved the organizational ability to conduct penetration testing and vulnerability analysis. The Agency infrastructure subject to assessment is comprised of over 8,000 systems, which includes workstations, servers, mainframes, and other telecommunications equipment. Vulnerability assessments are conducted in accordance with established Agency procedures.

- All DIA systems and networks are required to complete a certification process in order to obtain an approval to operate. The certification process is an in-depth technical assessment and compliance verification. Both DCI and Department of Defense (DoD) policies for IA apply. In part of this process, DIA has conducted IA assessments of approximately 80 discrete systems between January 1998 and June 1999. Such systems are operated both internally and externally to DIA.

- DIA has formalized policy that describes IA roles and responsibilities from the Director down to individuals. Infrastructure security policies and procedure standard for internal and external have also been developed and promulgated in

the form of a publication. Examples of what the INFOSEC publication addresses are:

- ❑ Life Cycle Security

- ❑ Acquisition Procedures

- ❑ Certification and Accreditation Process

- ❑ Incident Reporting

- ❑ Malicious Code Prevention

- ❑ Portable Computers

- ❑ Security Guidelines for System Administrators

- ❑ Storage Media Control and Accounting Procedures

- ❑ Information Systems Maintenance Procedures

There are other policies implemented to ensure consistent IA capabilities throughout the information system infrastructure. These policies establish standards for security safeguards and requiring formal testing to confirm compliance. They are also in parallel with DCI and DoD standards ensuring the confidentiality, integrity, and availability of systems. A configuration control and management board comprised of personnel from IA, communications security, and system management provides the final determination on the approval or disapproval of that system.

The aforementioned policies and procedures have been adequate in providing DIA with the necessary processes to secure and protect the Agency information infrastructure. We are, however, continuously challenged by the rapid technological change where no previous policy exists. For example, hand held palm top computers with impressive features (memory, processing power, etc.) have been introduced and are now in demand within our work environment. Handling of these devices and their use for information transfer between classified and unclassified environment compounded by the portability has become an issue. Another example is the introduction of multi-media technology that can record, digitize, and transmit video and audio information in the form of electronic data poses a challenge in terms of IA. We are continuously challenged by new technology to which no policy exists and at time, clashes with existing and outdated policies.

DIA has addressed the policy challenges of new technology by establishing a new function.

- • DIA has designated a function in the IA mission: New Technology Assessment. A team of IA professionals has the role of evaluating new technologies and providing conclusions and recommendations on the risk associated with their introduction. Conclusions and recommendations are presented to the CIO for decision. This approach has improved our engagement with the pace of new technology and enabled the CIO to make security knowledgeable and effective decisions.

- DIA has reviewed several IA products and technologies to enhance Agency information systems security capabilities for classified and unclassified environments. DIA identified several goals and objectives for IA improvements to drive the need and types of security capabilities required to protect the information system infrastructure. Objectives are:

  ❑ Implement an intrusion detection system

  ❑ Conduct forensic analysis of system anomalies and distinguish an attack from a system malfunction

  ❑ Acquire technologies to enhance vulnerability and penetration assessments

  ❑ Improve education and awareness of IA

- DIA is implementing an intrusion detection system to provide IA capabilities for monitoring the SCI enterprise. DIA is also upgrading the unclassified infrastructure that will introduce a single point of entry/exit via protected firewalls and other IA safeguards.

2.4.12. Defense Threat Reduction Agency

The Defense Threat Reduction Agency (DTRA), formed through fusion of three legacy agencies[11] and portions of the earlier Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Systems office, has focused extensive efforts on IA. In safeguarding DTRA internal assets, networks, and information has melded all of the best practices for IA from each of the legacy organizations, creating a safe and secure operational environment.

- As a part of DTRA's vulnerability assessment programs, a serious issue concerning the availability of sensitive unclassified, information about DoD programs on the Internet was elevated to the senior management. The Agency briefed this assessment, called Chessmaster, to Deputy Secretary of Defense and recommended a strategy for changing the way DoD uses the Internet. The Deputy Secretary of Defense implemented the recommended strategy and published a DoD interim memorandum. DTRA personnel participated in the development of a new Web Policy that was finalized on December 7, 1998. Agency personnel also participated in the writing of the new Website Administration Directive, which was released for comment in June 1999. At the personal request of Deputy Secretary of Defense, DTRA repackaged the Chessmaster assessment briefing as a web security awareness program for all senior executives and flag-level officers in the Department. This awareness briefing was provided to over 250 audiences comprised of 4,600. Briefings also were provided to senior leadership in OMB, National Security Council, the

---

[11] In October 1998, the Defense Special Weapons Agency, the On-site Inspection Agency, the Defense Technology Security Administration, and operational components of the ATSD (NCB) were merged to create the Defense Threat Reduction Agency.

White House, Federal Emergency Management Agency, and Department of Energy. The awareness program, coupled with the modifications in web usage, has significantly reduced the availability on the Internet of sensitive data about DoD programs and activities.

- Only NSA- and/or NIST-evaluated products appropriate for firewalls, remote access support and guard devices were used to establish the new DTRA networks. Through use of a smart card and VPN technology for remote access, DTRA has protected its information channels for its sensitive, unclassified networks with leading edge technology. This will be enhanced and expanded in 2000 and 2001. By migrating all administrative servers and user workstations to the NT 4.0 operating system configured at the C2 security level, DTRA has minimized both the external and insider threat to its information flows and repositories.

- In addition to thoroughly scrubbing its externally accessible web servers for excessive operational information, DTRA has instituted comprehensive safeguards against the seepage of sensitive, unclassified information.

- In FY2000 and 2001, DTRA plans to build upon the experience and database resources assembled for the Year 2000 effort for accreditation management of its mission critical and mission essential systems. During this period, DTRA will implement a more comprehensive and robust remote access system for both sensitive unclassified, and classified networks. DTRA will also conduct an extensive training and certification program in IA practices for its systems staff and user community.

For FY 2001 through FY 2005, DTRA will also need to implement the various emerging IA technologies now undergoing finalization for DoD-wide use, to include: 1) Fortezza-enabled smart cards for access to its networks, applications and databases, 2) the next generation network firewalls, and the 3) computer network defense concepts and systems. Currently much of this requirement is unfunded and must be addressed in the next DTRA budget opportunity.

In the area of vulnerability assessments, DTRA will continue in its role as a DoD-level resource, incorporating IA considerations into its regularly-scheduled assessments of DoD sites and organizations.

2.4.13. Defense Security Service

The Defense Security Service's (DSS's) strategy for IA combines products and services from the private and public sectors in a balanced approach for the protection of information assets that DSS is charged with protecting. A full time staff of professionals is responsible for ensuring that DSS's strategy for IA remains viable and is enforced to the greatest extent possible. Some of the steps that DSS has taken in the execution of its IA strategy include:

- Installing commercially available firewalls at the perimeter of the DSS network, monitoring network activity through these firewalls, and maintaining the firewalls

by ensuring that the latest software patches that address newly discovered vulnerabilities are installed.

- Implementing a Virtual Private Network capability between trusted users whom reside outside of DSS's network and DSS firewalls, which gives these users a protected channel to access to DSS's information assets.

- Requiring all DSS users to install virus-scanning software and maintain updated virus signature files for this software.

- Fielding a DoD PKI infrastructure within DSS which provides the ability to digitally sign and encrypt electronic communication within DSS and between DSS and its corporate partners.

- Installing an intrusion detection capability at strategic points in DSS's network, monitoring the network for suspicious activity, and taking steps to ensure that the potential attacks are quickly responded to and the damage is limited.

- Implementing in-house red and blue teams that test DSS's network defenses on a continuing basis and implement countermeasures to correct weaknesses that are discovered

- Implementing an in-house incident response, tracking, and reporting capability that is designed to keep track of anomalous behaviors, new vulnerabilities that are identified and reporting network incidents to the proper officials.

2.4.14. Army National Guard

The Army Reserve and National Guard (ARNG) IA initiatives are to enhance Army information operation capabilities. ARNG has put into operation the Department of the Army (DA) Network Security Improvement Program (NISP) in which the installation of firewalls (Gauntlet UNIX- Sun Ultra 10 workstations) and IDS at 60 Guard locations, the use of DoD/DA anti-virus software, and web page security. Implementation of IAVA compliance reporting, registration of ARNG POCs on ACERT list server and Army on-line (IA web page). The ARNG has been increasingly involved in the IA training arena, ARNG CERT certification, IA Level I and II certification for systems administrators, COMSEC custodian and command COMSEC inspector training, ISSM/ISSO training, and ARNG IA awareness training for users and information systems monitoring awareness training.

The following is a breakdown of the ARNG implementation of IO sections.

- 1.) ARNG Brigade IO Sections
  15 states authorized, 7 states manned New York, Hawaii, North Carolina, Arkansas, Oregon, Georgia, Idaho

- 2.) ARNG Division IO Sections
  8 states authorized, 6 states manned Kansas, Ohio, California, New York, Texas, Minnesota

- 3.) ARNG Field Support Teams
  7 states manned, Iowa, Maryland, Massachusetts, Texas, Vermont, Washington, Virginia

- 4.) ARNG Vulnerability Assessment Teams
  3 states authorized Virginia, Vermont, Washington

2.4.15. National Imagery and Mapping Agency

The NIMA continues to develop and refine an integrated and operational Infrastructure and IA Program, which will ensure the agency's ability to provide customers assured imagery, imagery intelligence, and geospatial information, consistent with the Defense IA Program. Significant NIMA IA initiatives over the past year include the development of a structured IA program, the establishment of a Critical Information and Infrastructure Protection Office, and the identification and development of CND functions. The NIMA Chief Information Officer (CIO) will continue to ensure the infrastructure and IA program remains a priority activity based on both DoD and IC guidance.

The NIMA program and operational implementation is organized into the following sub-elements:

- Infrastructure and IA Policy and Coordination

- Critical Infrastructure Protection

- Information System (IS) C&A

- Computer Network Defense (CND)

- Information System Security Officer / Manager Activities

- Public Key Infrastructure (PKI)

- Incident Investigation and Response

- IA Awareness, Training, and Certification

- Systems Security Engineering

- COMSEC

2.4.16. Special Communities

2.4.16.1. Health Affairs

The Assistant Secretary of Defense (Health Affairs) (ASD(HA)) IA goals are to protect the readiness information of our warfighters and the privacy of our beneficiaries. ASD(HA) has accomplished a number of actions to improve the DoD Medical Community's IA posture:

- Increased the number of IA support personnel (contractor staff) at Program Office level from 10 to 20 to improve the organization's ability to conduct risk assessments, penetration testing, and provide IA support services to Medical Facilities.

- Conducted certification and accreditation of all major medical information systems utilizing the DITSCAP methodology.

- Conducted on-line IA certification training to 90% of Health Affairs/TRICARE Management Activity staff prior to required implementation date. In conjunction with IA training, Health Affairs training includes Privacy Act information. Future IA certification will include information on the security/privacy requirements outlined in the Health Insurance Portability Accountability Act.

- Implemented planning for PKI to ensure all Health Affairs sharing partners will be interoperable with the DoD PKI program. Major sharing partners include Department of Veterans Affairs, Veterans Health Administration, Indian Health Service, National Institute of Health and numerous Manage Care Support Contractors. Increased participation in DoD and Medical Industry PKI meetings to facilitate interoperability between organizations.

- DiD technology and tools such as intrusion detection, VPN, and encryption are currently being used or put in place to improve information protection between trusted sharing partners.

- Developed an ASD(HA) enterprise-wide IAVA tracking and reporting processed called the Military Health System Computer Emergency Response Team (CERT). This program ensures that all advisories/patches are implemented and reported back to DoD and the Services. Implemented anti-virus software at mail server level as well as the workstation level.

2.4.16.2. Joint Electronic Commerce Program Office

The Joint Electronic Commerce Program Office (JECPO) is involved in providing guidance on IA and services to meet the needs of the DoD Components and JECPO in development and sustainment of e-business applications.

In most cases, adequate IA requires multiple solutions. To address this need, DoD is moving toward the DiD concept. JECPO is supporting DiD through the following activities: IA COTS products research; guidance to JECPO stakeholders on IA tools/solutions, regulations, and policies associated with e-business applications; coordination of the implementation of PKI across DoD e-business applications; and access control development for e-Portal Project.

2.4.16.2.1. IA COTS Products Research

Use of commercial security products and systems leads to economies of scale for DoD e-Business, and the Department benefits from sharing a common base of products with the private sector. The private sector is moving rapidly to electronic commerce and its demand for security products has created an increase in both the quantity and quality of commercial

secure e-business products. Current JECPO efforts in COTS products research include evaluation of digital signature products.

As other IA solutions emerge and as DoD expresses a need for IA solutions for e-Business, JECPO expects to be involved in evaluation of COTS products to continue helping to integrate state-of-the-art technology and to provide interoperability of systems throughout the enterprise.

2.4.16.2.2. Guidance to JECPO Stakeholders

JECPO's role as a clearinghouse for IA information on IA tools and solutions, regulations, and policies associated with e-business applications is increasing as the need for IA information is increasing throughout the DoD e-business community. Currently, most of the guidance JECPO provides is directly to the JECPO managers and to the Components at their request. That role will be expanding to include the following:

- Information Assurance Awareness

- System Security Vulnerability Analysis Process

- EB/EC Security Guiding Principles

- EB/EC Security Decision Support Tool

2.4.16.2.3. Coordination of e-Business PKI Implementation

For this pilot effort, JECPO: 1) assists DoD e-business project managers in identifying applications that require PKI enabling; 2) after the Components have developed their deployment schedule for PKI within each application, JECPO identifies user community requiring certificates; 3) develops certificate issuance plan for DoD and non-DoD entities; and 4) coordinates certificate issuance with the Components and the IECA.

2.4.16.2.4. Access Control Development for e-Portal Project

JECPO plays a key role in IA for the e-Portal Project. The e-Portal project will provide the end user with a single EB application access/registration portal an process for Government and non-Government organizations and personnel to facilitate DoD e-business. This new e-Portal will offer users a level of convenience that is currently unavailable, will support security practice, and will reduce administration costs by providing a centralized single sign-on infrastructure.

2.4.16.3. National Security Space Architect

The National Security Space Architect conducted an IA data collection effort under the auspices of the Mission Information Management Study. Data was collected through personal interviews, documentation and Internet searches with the pto capture the 2010 Evolved Baseline of IA for DoD and IC using the C4ISR Framework v2.0. The goal was to identify the existing IA efforts using a top down approach. The end product was a

document and brief consisting of IA definitions, key IA technologies/techniques, architectural views, issues and deficiencies, key references, and key POCs.

Major IA issues and deficiencies were categorized into policy, organizational, architectural, technical, and programmatic. Some policy issues identified include roles and responsibilities of government and the private sector. The private sector must address protection against common-place intrusions, theft and fraud, and how the federal government and private sector should address state-sponsored terrorism or hostile attack. The development of standards may support infrastructure protection but who develops them and how they are enforced must be addressed. The government may explore providing incentives for the private sector to invest in infrastructure protection much like the CRAF model. There is a need to identify what will encourage companies to address vulnerabilities.

The three major issues identified for the organizational bin are system administrator and personnel training, emergency reaction capability and situation awareness, and IA integration. Training and certification are necessary to ensure a first line of defense against information attacks. There is no consistent IA training for system administrators and personnel. Emergency reaction capability and situational awareness, the ability to determine system vulnerabilities and monitor fixes in real-time, must assist to control damage resulting from an attack and restore the protected information environment

The major architectural issues identified in the data collection effort was Multilevel Security (MLS). MLS is a risk-management issue that must provide a balance between community-wide needs and capability of system. Many architectures for the future still assume that MLS will be available.

The major technology issue identified was a lack of IA metrics. IA metrics is a continuing problem. There are no consistent widely recognized measures to evaluate IA techniques/technology. Thus, there is a need to develop community-wide IA measures for architecture development.

2.4.16.4. Unified Cryptologic Architecture Office

The mission of the UCA is to ensure Information Superiority for America and its allies. The implementation of the UCA and the Unified Cryptologic System (UCS) is driven by four overarching goals that support Joint Vision 2010, the DCI Strategic Intent, and the National Cryptologic Strategy for the 21st Century (NCS-21). These are to provide valued intelligence information to our customers; ensure an agile, collaborative, and interoperable cryptologic process; modernize and protect against the changing threat; and provide technically skilled, knowledgeable, innovative human resources. The Expanded Community Management Review Group (ECMRG) has oversight responsibility for the UCA, and is chaired by the Director, NSA, in his capacity as Community Functional Lead (CFL) for the cryptologic community.

The Unified Cryptologic Architecture Office (UCAO) is the CFL's staff for development and implementation of the UCA and UCS. Its priority is to make implementation of the UCA a fully-integrated cryptologic community activity. The UCAO role is to facilitate understanding of the UCA among the cryptologic community members and partners, and to guide, coordinate, and assess progress as the community moves forward to implement the

UCA vision. Implementation is the responsibility of the individual members and partners who together control the assets and resources that will make the future UCS a reality.

Significant advances toward the incorporation of IA into the UCA were made by the UCAO in 1999. The major accomplishments are detailed below.

- IA was established as a UCA functional area, with the primary purpose of protecting the cryptologic enterprise through layers of protect, detect, react, and recover mechanisms implemented in accordance with a DiD strategy. Countermeasures will span the scales of the WAN down to the desktop, and will include personnel, technical, and operational mechanisms.

- The Common Information Infrastructure Community Integrated Product Team (CII CIPT) issued its final transition report in July 1999. Several key IA recommendations were put forth, including:

  - The IC CIO should be responsible for IT associated with SCI.

  - The DoD CIO should be responsible for IT associated with Top Secret and below.

  - Information flowing from a higher to a lower classification enclave is the responsibility of CIO of higher enclave.

  - Collection systems should be treated as unprotected Internet portals.

  - Collected data entering trusted systems be filtered and sterilized.

  - Existing policy that SCI be the exception, not the rule, should be enforced. Cultural issues that thwart this policy must be overcome.

- The issue of enhanced dissemination of intelligence products at the collateral level to end users whose clearance levels rarely exceed Secret was explored in depth. The UCAO endorsed the March 1999 recommendations of the Intelligence Community Collateral Support Task Force, which include:

  - Write for the consumer

  - Implement need-to-know

  - Implement automatic marking and labeling

  - Revise training

- IA requirements were substantially incorporated into the Common Capstone Requirements Document (CRD) and the Cryptologic Planning and Programming Guidance (CPPG) document. The CRD addresses the cryptologic requirements of the IC and DoD. The CPPG prescribes the overarching community guidelines for building the FY 2002-2007 program as applicable to cryptologic resources, and summarizes key aspects of external guidance (the National Security Strategy, National Military Strategy,

the DCI Strategic Intent, etc.) that is applicable to the Cryptologic community.

2.4.17. Legislation

During 1999, there were several legislative and regulatory proposals that touch and concern Defense IA. These initiatives were primarily concerned with the export of Defense-interest technologies, and the maintenance of computer security. Each is summarized in the following paragraphs.

2.4.17.1. Export Initiatives Involving Defense-interest Technologies

Congress has introduced three bills, and the Administration has announced a new regulation, all of which seek to liberalize the export of Defense-interest technologies. While not specifically addressing IA, two of these bills and the regulation focus on the export of encryption technology; the other bill would authorize controls on exports of technology that protect Defense information. These are discussed in the following three sections.

2.4.17.1.1. Encryption Export

2.4.17.1.1.1. Background

Encryption hardware and software products electronically encode data for security purposes. Governments, financial institutions, and corporations routinely rely upon encrypted communications to conduct their daily business; so do individuals whose interests are hostile to the public safety and national security interests of the United States. For this reason, the unregulated export of sophisticated encryption products raises public safety and national security issues.

The market for encryption hardware and software is expanding rapidly. The U.S. is the primary developer and manufacturer of sophisticated encryption products, but overseas competitors are closing the gap. U.S. manufacturers complain that current export regulations prevent American producers from competing effectively in overseas markets. The regulatory prohibitions and exceptions, coupled with time-line and reporting requirements, allegedly render technically superior American products non-competitive. The Administration and Congress are listening.

If parties hostile to the interests of the United States have access to strong encryption products, not only can they hide their illicit activities, they might corrupt Defense information, compromise Defense systems, or interfere with Defense missions. For these reasons, DoD is concerned about the proliferation of strong encryption abroad.

The Department of Commerce currently manages the export of encryption items through the same regulatory structure that controls the export of other dual-use items – those products with military, strategic, or proliferation applications, and ordinary commercial uses. There is no restriction against the use of any encryption items within the United States. Whereas the U.S. freely exports "weak" encryption products, it restricts the export of more powerful encryption items -- that is, those products that are not easily compromised. The

U.S. frequently exports very strong encryption products on a carefully regulated, exception basis.

However, if foreign customers are turning to foreign competitors to meet their encryption requirements, then it is in the best interests of the United States to make American products more easily available to those foreign customers. Toward this end, Congress has introduced two bills -- H.R. 850 and S. 789 -- and the Administration has announced a new encryption export policy. All three initiatives would substantially relax U.S. encryption export restrictions. The Department of Defense has provided comments to Congress on all three proposals.

2.4.17.1.1.2. H.R. 850 and S. 789

Two legislative initiatives that seek to respond to industries' encryption export complaints are H.R. 850, the Security and Freedom Through Encryption (SAFE) Act of 1999 sponsored by Representative Goodlatte (R-VA) and S. 789, the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999 sponsored by Senator McCain (R-AZ).) Each represents unique legislation that removes encryption export control from the regulatory framework that currently governs the export of dual-use items.

Both the Goodlatte and the McCain bills permit the unregulated export of strong encryption technologies within the very near future. Yet neither bill sufficiently resolves the national security and public safety issues raised by the unregulated export and proliferation of strong encryption products. Senator McCain's encryption bill is more sympathetic to national security and public safety concerns than Representative Goodlatte's bill; however, neither bill is acceptable to the Departments of Defense, Justice (including the FBI), Commerce, State, Treasury, or the National Security Council.

Therefore, representatives from the Department of Defense met with and testified before Members of the House and Senate to explain DoD encryption proliferation concerns. In January 2000, the Administration published new interim final encryption export regulations. Both bills are on hold pending the outcome of the final regulations that will be published later in the year.

2.4.17.1.1.3. Revised and New Regulations and Policy

Late last year, the Administration promulgated new regulations that relaxed encryption export restrictions. However, to balance the requirements of industry and national security, the Administration reviewed these regulations again, and proposed a new regulatory framework to meet U.S. industry's global competition requirements, yet continue to provide essential public safety and national security protections.

The Administration favors a regulatory approach managed by the Executive Branch over a statutory approach. A regulatory scheme permits a more rapid response to stakeholders' requirements and permits more direct participation by government and private sector stakeholders. With others, the Department of Defense is a major contributor to the Administration's initiative.

The proposed framework rests on three principles: (1) a one-time technical review of encryption products in advance of sale, (2) a streamlined post-export reporting system, and

(3) a process whereby the government reviews exports of strong encryption to foreign government and military organizations, and to nations of concern. Consistent with these principles, the government agreed to update and simplify encryption export controls to permit the export of any encryption product, without a license and after a technical review, to commercial firms and other non-government end users in any country except the so-called "T-7" countries that support terrorism. In addition, telecommunications and Internet service providers could use encryption products to provide services to commercial firms and non-government end users. Previous liberalization for banks, financial institutions, and other approved sectors would be subsumed under this scheme. Interim final regulations were published in January 2000, and final regulations are expected later this year.

2.4.17.1.2. Export Administration.

S. 1712 was introduced in the Senate to authorize a new Export Administration Act governing exports of dual-use technologies, including those of relevance to the Department's IA program. While not specifically addressing IA, this legislation would authorize controls on exports of technology that protect Defense information. DoD included Defense IA requirements in its comments on the proposed bill and briefed to concerned members of Congress.

2.4.17.2. Computer Security Legislation.

Two additional bills relevant to Defense IA are H.R. 2413, the Computer Security Enhancement Act of 1999, and S. 1993, the Government Information Security Act of 1999. Both bills address the security of Government data and computer networks, and is therefore relevant to the Defense IA.

H.R. 2413 seeks to authorize and appropriate additional funds to the NIST to facilitate improvements in the Government's computer security regime. The explicit purpose of the bill is twofold: (1) to reinforce the role of NIST to ensure the security of unclassified information in Government computer systems; and (2) to promote technology solutions based on private sector offerings to protect the security of Federal computer systems. DoD is supporting House staffers to ensure that the bill reflects DoD's IA requirements.

S. 1993 seeks to strengthen the Office of Management and Budget's information security responsibilities, and clarify roles among Federal agencies to improve government information security. This bill would put in place a management structure for the implementation of risk-based computer security measures across the government. The bill assigns various roles and responsibilities to the Departments of Commerce and Justice, the General Services Administration, the Office of Personnel Management, and agencies' Inspector Generals and Chief Information Officers.

S. 1993 was introduced just before the Thanksgiving break. DoD representatives have met with Senate staffers to discuss DoD's IA requirements within the context of this bill.

2.5. Assessment of the DIAP

Critical deficiencies and shortfalls generally can be identified with technology, operations or people. The following discussions illustrate the DIAP office functional area viewpoints and activities that address past and current concerns and provide an indication of intentions for the future.

2.5.1. Critical Deficiencies and Shortfalls

The preceding sections of the report highlight the significant IA activities and processes achieved and implemented throughout DoD in 1999. Each of these accomplishments is a necessary step along the path towards a fully protected, reliable, and available Defensive information infrastructure in support of the warfighting and business missions. Although the Department witnessed major IA gains, there remain a number of critical deficiencies and shortfalls in the overall program. The most critical deficiency that affects all areas is the insufficient commitment of funding required to implement and operate a robust IA program while continuing to research, explore, and develop advanced and promising technologies. In an era of constrained budgets and ever more challenging prioritization problems, the immediate operational priorities frequently take priority over long-term investments, and IA is no exception. This situation produces short-term solutions that may, in the long run, exacerbate long-standing problem areas. The following sections address nine areas requiring additional programmatic, policy, and legislative resources.

2.5.1.1. Human Resources

In no area is insufficient funding more evident than in IA human resources. As previously mentioned, an IPT already has identified serious, long-standing problems in the training, retention, and management of IA personnel. Not only are there not enough of them, but many of those available lack adequate training and the DoD is experiencing an attrition of these individuals almost as fast as it can train them.

A partial solution lies in outsourcing because the Department may never be able to attract and retain sufficient numbers of skilled personnel in these areas. Unfortunately, this solution brings with it added risk in that individuals working on our systems are no longer Department employees, but contractors, whose loyalties may lay elsewhere. Exacerbating this particular problem is the fact that Contracting Officers and those developing the Statements of Work (SOW) for these contractors are rarely IA experts and fail to include sufficient safeguards in the SOW so that contractor personnel are screened as carefully as are DoD employees. This problem is particularly prevalent among those information systems that fall under the category of "sensitive unclassified". Classified systems normally have such requirements already built in.

The problem of insufficient numbers of trained people is a consequence of the "do more with less" mindset as well as the promise of saving manpower by automating. There clearly is a savings of personnel when manual data entry and analysis activities are automated, but inadequate attention has been paid to the numbers and types of manpower necessary to manage and provide security for these systems. Little analysis has been done on the appropriate numbers of people needed to perform these functions, although much is available on the types of skills (at least in the private sector). In many cases, these functions

are performed by individuals who have other primary duties, exacerbating the accounting of who does what. Additional study is needed to document the manning requirements as well as skill levels required.

Finally, the continuing issue of inadequate IA and IT training across all agencies is cited in report after report. If the Department were to apply the best practices from the common, yet important, processes of a personnel safety program, IA training would occur at entry/accession points, at appropriate career points throughout Department service, and as specialized training for those with specialized responsibilities in IA. As the Department has discovered, often following an unnecessary loss of life, safety training must be fully integrated into the Department's way of doing business. Similarly, if the Department is going to control its IA arena, then the Department must make IA training an integral part of the Department's way of doing business. Much has been done to date to provide the most critically needed training, but much more needs to be accomplished to make it a way of life.

2.5.1.2. Policy Integration

Policy vacuums, outdated policies, and conflicting policies require constant attention; yet this is one of the more difficult areas to address. We must strike a balance between not enough policy and too much policy because not every situation can be addressed and policy generally lags behind new technology. Policies frequently drive operations - either by enhancing or making things unnecessarily more difficult. The IA challenge is to provide a policy framework sufficient to foster good decisions and clarify the roles and responsibilities of the various levels of organization. Frequently, however, in the IA arena, good policy is difficult to develop because there is no clear path, just a weighing of risks, benefits, and the least destructive/painful alternative.

2.5.1.3. Operational Environment

Much improvement has occurred over the last year to provide visibility into the Department's networks. The Services and most of the Agencies have made significant investments in redesigning their networks, developing policies, procedures and guidelines, and purchasing and installing appropriate security devices (firewalls, IDS, etc.). Unfortunately, this effort is uneven across the Department, and many of the smaller Agencies have yet to get control over their networks. Lessons learned from the Y2K efforts are assisting in this endeavor, but much remains to be done.

2.5.1.4. Readiness Assessment

To determine how effective the Department's IA practices are, the DIAP must be able to predict with some degree of confidence how well those practices will protect our information technology resources against unknown threats. The DIAP is developing an IA readiness assessment capability to meet this challenge.

First, there is an inherent divergence in orientation and competence with regard to consideration of readiness, as viewed from a warfighter's perspective, and as viewed from an information technologist's perspective. The DIAP is striving to bridge that gap by "operationalizing" information assurance readiness within the Defense community. Several

activities have been undertaken to forge this evolution, including development of: a definition of IA readiness in an operational context; a comprehensive set of metrics for measuring IA readiness; standard criteria to be used in applying the metrics; and requirements and methodologies for collecting and analyzing metrics data.

Second, the development of IA readiness metrics has been hampered by a lack of existing relevant information on system security metrics. The civilian sector is now addressing the topic through industry forums, and some forums are developing models and criteria they hope to get approved as industry standards. The DIAP is participating in civilian and government forums to cross-fertilize their respective efforts. In spite of the dearth of relevant information currently available, the DIAP began distributing a first round of proposed metrics to early collaborators for comment. The plan is to systematically increase both the fidelity of the metrics and diversity of collaborators, before beginning an informal coordination process this spring.

The approach to developing the IA readiness definition and metrics involves extensive research and collaboration with people from diverse specialties with IA expertise, operational expertise, and metrics expertise. Through collaborative efforts, the DIAP is developing a range of metrics that collectively represent the five attributes of IA (integrity, availability, authentication, confidentiality, non-repudiation), and link the assets being measured to some warfighting capability. This will enable the DIAP to draw an effective picture of how the Department's IA stature can be expected to affect the ability to successfully prosecute any combat or peacekeeping mission. Thus, after the complete implementation of an IA readiness assessment capability, the Department will be depicting the value of information being protected by IA directly to a warfighting capability.

2.5.1.5. Acquisition

There are many challenges for the DoD in the acquisition arena. One of the challenges includes the impact of Acquisition Reform on the acquisition process and how to ensure proper oversight, as well as appropriate interjection of IA into the process. Acquisition policy must be reviewed and associated training developed for program managers to ensure awareness and appropriate tools and methodologies are available. The other challenge is the acquisition of IA tools and products. First, these tools and products must be certified in a fair, timely process. Second, there must be a way to distinguish between similar products to assess which is best for a particular network environment. Third, policy must require that these certified products are the only ones approved for use within the DoD. The pace of technology argues that both challenges be addressed in a timeframe that the DoD acquisition systems must accommodate.

2.5.1.6. Architecture

The issues and difficulties of developing IA architectures are addressed in section 2.2.12.

2.5.1.7. Research and Technology

The research and technology efforts of the department are on track and making progress toward a coherent research and technology investment program justification. However, funding is not keeping pace with demands.

2.5.1.8. Security Management

Essentially not addressed but a major area for resolution in 2000, if continued progress and evolution toward a coherent and comprehensive IA program and programmatics is to be achieved.

2.5.1.9. Law Enforcement and Counterintelligence Liaison

DoD Law Enforcement and Counterintelligence Organizations (DLECO) play a critical role in responding to computer intrusions. It is critical that DLECOs coordinate their investigations and operations in this arena within DoD as well as with their civilian agency counterparts. Intruders do not single out a Service as a target. Generally an intrusion into one Service or Agency system correlates to an intrusion in another. Although the DLECOs have taken the first step by creating a Law Enforcement/Counterintelligence cell in the JTF-CND to liaison these investigations and operations, current coordination is still severely lacking. To address this specific issue the DLECO community has formed the DLECO Operations Chief Working Group to address improving this coordination and support for the CND mission by better integrating the Law Enforcement/Counter Intelligence (LE/CI) communities into the processes of IA and CND.

THIS PAGE INTENTIONALLY LEFT BLANK

3. References

DoD Directive, S-3600.1, "Information Operations (IO) (U)," December 6, 1996

National Research Council, Computer Science and Telecommunications Board, "Realizing the Potential of C4I; Fundamental Challenges," 1999

Report to Congress, "Assessment of the Information Assurance Program of the Department of Defense," May 1998

"Secretary of Defense Report to the Congress on the Information Security Activities of the Department of Defense," November 15, 1997

Presidential Decision Directive (PDD) 63, "Critical Infrastructure Protection," May 22, 1998

PKI Implementation Plan for the DoD, Version 2, October 29, 1999

Program Decision Memorandum I (PDM I), August 13, 1999

Psychology Associates, Ltd., "Insider Threats to Critical Information Systems," Contract #98-G-7900, August 31, 1999

"Concept of Operations for the Joint Web Risk Assessment Cell (JWRAC)," February 12, 1999

"Information Assurance Red Team Handbook"

Chairman of the Joint Chiefs of Staff Instruction 6510.01B, "Defensive Information Operations Implementation," 22 August 1997 (includes CH-1, 26 August 1998

H.R. 850, "The Security and Freedom Through Encryption (SAFE) Act of 1999"

S. 789, "The Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999"

H.R. 2413, "The Computer Security Enhancement Act of 1999"

S. 1993, "The Government Information Security Act of 1999"

S. 1712, "Export Administration Act of 1999"

General Accounting Office Report GAO/AIMD-99-107, "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999

Chairman of the Joint Chiefs of Staff Memorandum CM-510-99, "Information Operations Condition (INFOCON)," 10 March 1999

Deputy Secretary of Defense Memorandum, "Management of the Department of Defense Information Assurance Program," January 30, 1998

Deputy Secretary of Defense Memorandum, "Website Administration," December 7, 1998

Deputy Secretary of Defense Memorandum, "DoD Information Assurance Vulnerability Alert (IAVA)," December 30, 1999

Assistant Secretary of Defense (C3I) Memorandum, "Defense-wide Information Assurance Implementation Plan," February 12, 1999

Assistant Secretary of Defense (C3I) Memorandum, "Assignment of Program Management Office Responsibilities for the Department of Defense Public Key Infrastructure (PKI)," April 9, 1999

Assistant Secretary of Defense (C3I) Report, "DoD CIO Annual Information Assurance Report," May 1999

DoD Chief Information Officer, "DoD Information Management (IM) Strategic Plan," Version 2.0, October 19, 1999

"Defense-Information Assurance Red Team Methodology," May 1999

"Public Key Infrastructure Roadmap for the Department of Defense," Version 3.0, October 29, 1999

"X.509 Certificate Policy," Version 4.0, October 29, 1999

"Public Key Infrastructure Implementation Plan," Version 1.0, Rev G3, September 1999

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

DoD Directive C-5200.5, "Communications Security (COMSEC)(U)," April 21, 1990

DoD 5200-28-M, "ADP Security Manual," January 1973 and Change 1, June 24, 1979

Information Assurance and Information Technology Human Resources Integrated Process Team, "Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense," August 27, 1999

National Security Agency, "Information Assurance Technical Framework," Release 2.0.1, September 1999

Additional Important IA and IA-related Bibliographic Materials.

In addition, the following reports provide background on the importance of IA to national security in both the broadest terms and with respect to specific responsibilities and equities. They are:

National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990

The Report of the Joint Security Commission, "Redefining Security," February 28, 1994

The Report of the Joint Security Commission II, August 24, 1999

General Accounting Office Report GAO/AIMD-96-84, "Computer Attacks at the Department Pose Increasing Risks," May 1996

General Accounting Office Report GAO/NSIAD-98-132R, "DoD's Information Assurance Efforts," June 1998

Defense Science Board Task Force Report "Information Warfare-Defense, November 1996

The Report of the DoD Information Assurance Task Force, "Improving Information Assurance: A General Assessment and Comprehensive Approach to an Integrated IA Program for the Department of Defense," March 28, 1997

Deputy Secretary of Defense Memorandum, "Department of Defense Reform Initiative #27 - DoD Computer Forensics Laboratory and Training Program," February 10, 1998

Deputy Secretary of Defense Memorandum, "Information Vulnerability and the Worldwide Web," September 24, 1998

Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," May 6, 1999

Deputy Secretary of Defense Memorandum, "Smart Card Adoption and Implementation," November 10, 1999

Assistant Secretary of Defense (C3I) Memorandum, "Interim Guidance for the Department of Defense (DoD) Public Key Infrastructure (PKI)," August 11, 1998

"Certification Practices Statement for the Certificate Management Infrastructure of the Defense Information Infrastructure," Version 0.2, April 10, 1998

Director, Infrastructure and Information Assurance, OASD(C3I), "Computer Network Defense: Policy and Requirements," August-December 1999

Final Report of the Insider Threat Integrated Process Team, "DoD Insider Threat Mitigation Plan," December 27, 1999

Worldwide Web Security Training Guidance and Requirements Working Group Report, undated (draft)

THIS PAGE INTENTIONALLY LEFT BLANK

4. Acronyms and Abbreviations

ACC	Air Combat Command
ACTD	Advanced Concept Technology Demonstration
AFCERT	Air Force Computer Emergency Response Team
AFNOC	Air Force Network and Operations Center
AIDE	Automated Intrusion Detection Environment
AIDE-ACTD	Automated Intrusion Detection Environment Advanced Concept Technology Demonstration
AIS	Automated Information System
AOR	Area of Operations
APPN	Appropriation
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASIMS	Automated Security Incident Measurement System
ATM	Asynchronous Transfer Mode
A/V	anti-virus
BMDO	Ballistic Missile Defense Organization
C/S/A	CINC, Service and Agency
C2	command and control
C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computers
C4I	C4 and Intelligence
C&A	Certification and Accreditation
CA	Certification Authority
CAP	Connection Approval Process
CBT	computer-based training
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CINC	Commanders in Chief
CIO	Chief Information Office

CIP	Critical Infrastructure Protection
CIPP	Critical Infrastructure Protection Plan
CISD	C4I Integration Support Activity
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMI	Certificate Management Infrastructure
CNA	Computer Network Attack
CND	Computer Network Defense
COE	Common Operating Environment
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial-off-the-shelf
CP	Certificate Policy
CPS	Certificate Practice Statement
DA	Department of the Army
DARPA	Defense Advanced Research Projects Agency
DCFL	Defense Computer Forensics Laboratory
DCI	Director of Central Intelligence
DCITP	Defense Computer Investigation Training Program
DFAS	Defense Finance and Accounting System
DIA	Defense Intelligence Agency
DIAP	Defense-wide Information Assurance Program
D-IART	Defense-Information Assurance Red Team
DiD	Defense-in-Depth
DII	Defense Information Infrastructure
DIO	Defensive Information Operations
DIRNSA	Director, NSA
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITSCAP	DoD Information Technology Security Certification and Accreditation Process

DLA	Defense Logistics Agency
DLA CERT	Defense Logistics Agency Computer Emergency Response Team
DMS	Defense Messaging System
DNS	Domain Name Service
DoD	Department of Defense
DoN	Department of the Navy
DPSS	Defense Planning Support System
DSS	Defense Security Service
DTRA	Defense Threat Reduction Agency
EKMS	Electric Key Management System
ETA	education, training, and awareness
FBI	Federal Bureau of Investigation
FDD	First Digitized Division
FEA	Front End Assessment
FSO	Field Security Officer
FY	Fiscal Year
GCCS	Global Command Control System
GIG	Global Information Grid
GNIE	Global Network Information Enterprise
GNOSC	Global Network Operations and Security Center
GOTS	Government-off-the-shelf
G&PM	guidance and policy memorandum
IA	Information Assurance
IAG	Information Assurance Group
IATF	Information Assurance Technical Framework
IAVA	Information Assurance Vulnerability Alert
IBT	Internet-Based Training
IC	Intelligence Community
IDS	Intrusion Detection System
IG	Inspector General
IMDS	Intrusion Misuse and Deterrence System

INFOCON	Information Operations Condition
INFOSEC	Information Security
IO	Information Operations
IOTC	Information Operations Technology Center
IP	Internet Protocol
IPLAN	Implementation Plan
IPT	Integrated Process Team
IRC	INFOSEC Research Council
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISSP	Information Systems Security Policy
IT	Information Technology
IWF	Information Warfare Flight
J6	Joint Staff
JCAPS	Joint C4ISR Architecture Planning/Analysis Systems
JIDS	Joint Intrusion Detection System
JIOC	Joint Information Operations Center
JMRR	Joint Monthly Readiness Review
JSOC	Joint Special Operations Command
JTF-CND	Joint Task Force-Computer Network Defense
JWRAC	Joint Website Risk Assessment Cell
KMI	Key Management Infrastructure
LAN	Local Area Network
MAJCOM	Major Command (USAF)
MCEB	Military Communications-Electronics Board
MITNOC	Marine Corps Information Technology and Network Operations Center
MLS	Multilevel Security
MSL	Multiple Security Levels
N/MCI	Navy/Marine Corps Intranet
NCA	National Command Authorities

NCCs	Network Control Centers
NETOPS	Network Operations
NIAP	National Information Assurance Partnership
NIMA	National Imagery and Mapping Agency
NIPC	National Infrastructure Protection Center
NIPRNET	Sensitive Unclassified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NOSC	Network Operations and Security Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSIP	Network Security Improvement Program
OASD	Office of the Assistant Secretary of Defense
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
PDD	Presidential Decision Directive
PDM	Program Decision Memorandum
PEP	Program Execution Plan
PK	Public Key
PKI	Public Key Infrastructure
PMO	Program Management Office
POC	Point of Contact
POM	Program Objective Memoranda
PPBS	Planning, Programming, and Budgeting System
PROTECT	Promote Reliable On-Line Transactions to Encourage Commerce and Trade
RA	Reserve Affairs
RC	Reserve Components
RCERT	Regional CERT
RNOSCs	Regional Network Operations and Security Centers
ROE	Rules of Engagement
SA	System Administrator

SABI	Secret and Below Interoperability
SAFE	Security and Freedom through Encryption
SHADOW	Secondary Heuristic Analysis for Defensive On-Line Warfare
SII	Special Interest Item
SIPRNET	SECRET Internet Protocol Router Network
SMI	Security Management Infrastructure
SOW	Statement of Work
SRA	Security Research Alliance
STIG	Security Technical Implementation Guides
SWA	Secure Web Access
TCCC	Theater C4ISR Coordination Center
TNCC	Tactical Network Control Center
T-SABI	Top Secret and Below Interoperability
TTP	tactics, techniques, and procedures
UCA	Unified Cryptologic Architecture
UCAO	Unified Cryptologic Architecture Office
USCENTCOM	United States Central Command
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USEUCOM	United States European Command
USJFCOM	United States Joint Forces Command
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States Southern Command
USSPACECOM	United States Space Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command
VCTS	Vulnerability Compliance Tracking System
VPN	Virtual Private Network
WAN	Wide Area Network
WMD	Weapons of Mass Destruction
ZBR	Zero Base Review

Annex 1. GAO Reports

The following refer to GAO Reports (GAO/AIMD-99-107, Aug 26, 1999, "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk" and the GAO/AIMD-96-84, May 2, 1996 "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks" and the September 1996 Limited Official Use report GAO/AIMD-96-144).

1. Direct the DISA Director to expand the Security Readiness Review (SRR) process to include timely and independent verification of the corrective actions reported by DMCs or other responsible parties. (P4)

2. Direct the DoD CIO to ensure that the Defense-wide Information Assurance Program defines how its efforts will be coordinated with the Joint Task Force and other related initiatives. (P4)

3. Earlier recommendations confirmed GAO/AIMD-96-144, September 1996 empowering the DOD CIO to establish a comprehensive, department-wide information security program; ensuring that security programs of the military departments and Defense agencies are consistent with the department program; and periodically reporting on progress in improving controls over information security.

THIS PAGE INTENTIONALLY LEFT BLANK

Annex 2. National Research Council Recommendations

Recommendations for Information Systems Security

The following refer to the National Research Council Report on C4 Information Security.

S-1: The Secretary of Defense, through the Assistant Secretary of Defense for C3I and the Chairman of the Joint Chiefs of Staff, should designate an organization responsible for providing direct operational support for cyber-defense to commanders.

S-2: The Secretary of Defense should ensure that adequate information system security tools are available to all DoD civilian and military personnel, direct that all personnel be properly trained in the use of these tools, and then hold all personnel accountable for their information system security practices.

S-3: The Secretary of Defense, through the Assistant Secretary of Defense for C3I, the Chairman of the Joint Chiefs of Staff, and the CINCs, should support and fund a program to conduct frequent, unannounced penetration testing of deployed C4I systems.

S-4: The Assistant Secretary of Defense for C3I should mandate the immediate department-wide use of currently available network and configuration management tools and strong authentication mechanisms.

S-5: The Under Secretary of Defense for Acquisition and Technology and the Assistant Secretary of Defense for C3I should direct the appropriate defense agencies to develop new tools for information security.

S-6: The Chairman of the Joint Chiefs of Staff and the service Secretaries should direct that a significant portion of all tests and exercises involving DoD C4I systems be conducted under the assumption that they are connected to a compromised network.

S-7: The Secretary of Defense should take the lead in explaining the severe consequences for U. S. Military capabilities that arise from a purely passive defense of its C4I infrastructure and in exploring policy options to respond to these challenges.

THIS PAGE INTENTIONALLY LEFT BLANK

Annex 3. C3I Goals

Goal 1:   Ensure continuity of mission-essential DoD operations despite Y2K disruptions.

Goal 2:   Implement effective programs for establishing information assurance (IA) and critical infrastructure protection (CIP)

Goal 3:   Build a coherent global network

Goal 4:   Plan and implement joint and combined end-to-end C3ISR and space integration

Goal 5:   Promote the development of knowledge management and a skilled-based workforce throughout DoD

Goal 6:   Establish policies and procedures that will lead to the reinvention of intelligence for the 21st century

Goal 7:   Strengthen the information operations, security, and counterintelligence (CI) posture of the Department of Defense

Goal 8:   Promote electronic commerce and business process change throughout the DoD

Goal 9:   Foster development of an advanced technology plan for information superiority

Goal 10:   Transform OASD(C3I) into a caring, nurturing organization that is a model of the teamwork needed to realize all of the above goals.

THIS PAGE INTENTIONALLY LEFT BLANK

Annex 4. Goal Two

2. Implement Effective Programs for Establishing Information Assurance (IA) and Critical Infrastructure Protection .		
	2.1 Train and certify all appropriate personnel in security disciplines	
		2.1.1 Execute Manpower IPT Recommendations
		2.1.2 Certify Information System Users and Administrators
		2.1.3 Achieve FOC - DoD Computer Forensics Tng Cntr
		2.1.4 Integrate Personnel Security Policies with IA Rqmts
	2.2 Improve operations to provide secure operating environment throughout DoD	
		2.2.1 Integrate Intel and Reserve Community into DIAP
		2.2.2 Achieve FOC - DoD Computer Forensics Lab
		2.2.3 Improve Execution of IAVA Process
		2.2.4 Execute DoD PKI Strategy
		2.2.5 Integrate IA Policy - DoD and Federal
		2.2.6 Improve DoD WWW Security
		2.2.7 Develop Attack Sensing and Warning Strategy
		2.2.8 Establish Policy/Process to PKI-Enable Applications
		2.2.9 Develop GIG IA Architecture Overlay
	2.3 Leverage Innovations/Developments in IA/CIP Technology Solutions	
		2.3.1 Establish Process to Influence I&IA-Related R&D
		2.3.2 Develop Electronic Marking and Labeling Directive
		2.3.3 Develop COTS Policy Framework
	2.4 Identify and prioritize criticality and interdependence of information, people, and other assets and capabilities upon which DoD depends, enabling the effective allocation of CIP, Defensive IO, Security, and Counterintelligence resources to those most critical to the DoD.	
		2.4.1 Operationalize Critical Infrastructure Protection (CIP)
		2.4.2 Achieve IOC - Virtual CIP Integration Staff (CIPIS).
		2.4.3 Develop Information Systems Security Program (ISSP) Budget Framework and Prioritization Process

THIS PAGE INTENTIONALLY LEFT BLANK

Annex 5. Goal Four

Objective 4.1 - – Make IA an Integral Part of DoD Mission Readiness Criteria
Strategy 4.1.1 - – Designate all functions within the DII as either mission critical, mission essential or mission support.   DoD infrastructure owners (e.g., command and control, logistics and transportation, health affairs, intelligence, personnel, financial services), in coordination with the Joint Staff and the Critical Asset Assurance Program, shall identify those mission functions and information system elements of their infrastructures which perform mission critical, mission essential, or mission support functions.
Strategy 4.1.2 – -Provide information assurance levels consistent with the Department's mission critical, mission essential, and mission support requirements for all networks of the DoD Components and component elements of the DII.   Detailed assurance criteria for each level and interconnection between levels will be developed and specified.
Strategy 4.1.3 - – Integrate IA readiness standards and metrics into the DoD readiness reporting process.   Department IA policy must address the accountability aspects of IA. It must drive the availability resources required by operational commanders and others accountable for their use, and thus the Department's IA posture.

Objective 4.2 - – Enhance DoD Personnel IA Awareness and Capabilities
Strategy 4.2.1 - – Train and certify network managers, operators, systems administrators, and all other personnel involved in the operation and management of the DII and its component systems.   Training and certification must extend into the contractor community supporting DoD.
Strategy 4.2.2 - – Review and create (as needed) military and civilian career fields to ensure that they reflect adequate recognition of network information assurance skills and capabilities.   New career fields shall be established as necessary. Career field designation is essential to establishing ascension paths for the military and civilian disciplines critical to ensuring efficient secure operation of the DII.

Objective 4.3 - – Enhance DoD IA Operational Capabilities
Strategy 4.3.1 - – Protect the DII with a defined and controlled perimeter.   While DoD depends upon unclassified connections to the Internet to accomplish unclassified basic support functions and to provide access to open source information, these connections will be controlled and capable of being monitored. Interconnection of all classified systems with any other system will be accomplished by high assurance means. Authentication will be broadly employed.

Objective 4.3 - – Enhance DoD IA Operational Capabilities
Strategy 4.3.2 – Protect the DII with an integrated attack sensing and response management capability. As part of the integrated capability, all DoD Components and Component elements of the DII, and all access points into the DII, will have intrusion detection capabilities.
Strategy 4.3.3 – All DoD Components and component elements of the DII will adhere to establishe connection standards and procedures. All DII elements will provide the required levels of security configuration management, employ methods to detect unauthorized activity and malicious code, and have adequate provisions for continuity of operations and rapid reconstitution.
Strategy 4.3.4 – Implement "DiD" concepts across the DII. This concept will be applied to each operating assurance level and shall be applied in accordance with DoD criteria, including existing protective measures traditionally used to safeguard national security information. This strategy will consist of the following: • Hardened network infrastructure. • Protected host secure operating systems. • Protected enclave boundaries. • User/Application layer security services, including non-repudiation, signature, integrity, and confidentiality. • Employment of strong identification and authentication (I&A) services. • Use of a common, integrated DoD Public Key Infrastructure (PKI) to enable security services at multiple levels of assurance. • IA situational awareness based on both network and host monitoring to formulate and suppor an attack sensing and response management capability. • Approved high assurance devices and configurations for all interconnections among mission sensitivity levels.

Objective 4.4 – Establish an Integrated DoD Security Management Infrastructure (SMI)
Strategy 4.4.1 – Integrate a broad spectrum of network services (e.g., audit, intrusion detection, operational network monitoring and control) into the DoD SMI. Confidence in the secure operation of the DII must be grounded in a real-time understanding of network-wide activities. Further, the ability to identify when network users have gained access to unauthorized areas or information, or to be able to attribute specific network activity to specific users of the network is an important factor in dealing with the insider threat.
Strategy 4.4.2 – Implement the DoD PKI consistent with the May 6, 1999, policy memorandum, Do PKI Roadmap, DoD PKI Implementation Plan, and the DoD PKI Certificate Policy.

THIS PAGE INTENTIONALLY LEFT BLANK